Information Risk Management - Strategies and Rationale Promoting Appropriate Information Risk Management

UK National Security Strategy 2010 [1]

In October 2010 the Government's National Security Strategy set clear priorities and listed *'Cyber Attacks'* second after Terrorism in a *'complex range of threats'* or *'Tier One risks'* to UK national security.

The Strategy called *for 'a much closer relationship between government, the private sector and the public'*. The Strategy placed responsibility on business to work closely with government *'to strengthen our defence against cyber attack and to prepare for the worst, so that if it happens, we are able to recover rapidly and keep Britain moving'*. The Strategy warned that, like Terrorism, Cyber Attacks were not a risk for the future, but that the *'Government, the private sector and citizens are under sustained cyber attack today'*.

Strategic Defence and Security Review 2010 [2]

The Strategic Defence and Security Review (SDSR), which was also released by the Government in October 2010, also listed Cyber Security second after Counter-Terrorism as principle elements of the strategic policy. The Review reiterated that *'Over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially'*. An outcome of the SDSR was that the Government put in place a £650 million, four-year National Cyber Security Programme (NCSP).

NATO Lisbon Summit 2010 [3]

The November 2010 NATO Lisbon Summit highlighted the cyber domain as an area of significant new risk and opportunity for the Alliance. The new Strategic Concept for Defence and Security committed the Alliance to: *'develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations'*.

Cybersecurity Summit 2010 [4]

Speaking at the Worldwide Cybersecurity Summit in June 2011, Sir Michael Rake, chairman of BT Group, expressed the view that awareness of cyber crime and the necessity of protecting corporate

and personal data are not as highly prioritised at board level as they should be.

Sir Michael went on to say: *'Governance and risk management are familiar topics in the board room. It is therefore surprising that companies always feel under pressure to meet compliance deadlines of one type or another and often panic to implement solutions they believe will address the most visible, urgent or potentially costly to ignore regulation looming on the horizon, without even putting this into the context of the existing enterprise risk management framework. Many businesses are now on their second or third cycle of trying to automate processes related to compliance with specific policies, industry standards, and government regulations. With requirements evolving, companies find themselves with discrete solutions for PCI DSS, Data Protection, FSA, Sarbanes-Oxley, ISO27001 and others. Although these businesses have achieved some successes with their initial projects, much of the success has been short lived, and costly. More specifically, investments in information security get more and more difficult to secure as sustainability cannot be demonstrated to the board. And then you get the next high profile data breach...'*

Sir Michael concluded his speech by advocating five best-practice lessons:

- **Understand your risk profile:** Compliance requirements alone are no longer sufficient - businesses must look at their people, their processes as well as the technologies that can help them.
- **Make risk management your objective, compliance will come naturally.**
- **Avoid quick fixes and silos:** Organisations should facilitate the handling of short-term needs while providing a foundation for an integrated long-term solution that is flexible enough to support multiple regulations and new functionalities.
- **Automate:** Businesses should look for Governance, Risk and Compliance solutions that are easy to deploy, require no customisation and are simple to upgrade.
- **Educate:** Ensure training and education of staff and customers are firmly on the agenda.

Cyber Security Strategy 2011 [5]

In November 2011 The Rt Hon Francis Maude, Minister for the Cabinet Office, launched the first UK Cyber Security Strategy. The Strategy was an indirect response to the October 2010 National Security Strategy (discussed above) and a direct response to the SDSR (discussed above), which, as part of the NCSP, undertook for its provision. In the adjoining Written Ministerial Statement, the Minister referred to the overwhelming growth of the internet being the biggest social and technological change of his lifetime, and he felt that the growth was increasing the vulnerability to national security from the threat of *'organised criminals, terrorists, hostile states, and 'hacktivists''*. The Minister expressed a key aim and Objective 1 of the *'vision for UK cyber security in 2015'* as making *'the UK one of the most secure places in the world to do business'*.

The Strategy undertook to take a *'risk-based approach'*, but that this would be carried out *'working in partnership'* as much of the infrastructure at stake is owned and operated by the private sector, but that in order to progress with cyber security, the partnership needed to reach out multi-nationally.

Cyber Vision for 2015

The Minister's vision for 2015 is for a UK where:

Individuals:

- People know how to get themselves a basic level of protection against threats online.
- Individuals are careful about putting personal or sensitive information on the internet.
- Everyone, at home and at work, can help identify threats in cyberspace and report them
- Individuals play their part in transacting safely with businesses and Government
- People are clear that, as in the offline world, we are each responsible for our behaviour in cyberspace.

The private sector:

- Companies are aware of the threat and use cyberspace in a way that protects commercially sensitive information, intellectual property and customer data.
- Private organisations work in partnerships with each other, Government and law enforcement agencies, sharing information and resources, to transform the response to a common challenge, and actively deter the threats we face in cyberspace
- Companies capitalise on the growth in demand in the UK and globally for vibrant and innovative cyber security services.
- The private sector has built upon the strengths of the UK's skills base in cyber security to invest and

create centres of excellence to provide the cyber security skills we will need in future.

Government, where we have:

- Built up our capacity to detect and defeat high-end threats.
- Helped shape an international consensus on norms of behaviour in cyberspace.
- Reduced vulnerabilities in government systems and our critical national infrastructure.
- Grown the cadre of cyber security professionals.
- Strengthened law enforcement and tackled cyber crime.
- Improved prevention and public awareness.
- Raised business awareness.
- Seized the business opportunities – working with industry and academia to boost our share of the cyber security market and cemented the UK's status as a safe place to do business online.

GCHQ's '10 Steps to Cyber Security' [6]

In September 2012, Iain Lobban, Director of the Government Communications Headquarters (GCHQ), on behalf of the Government and intelligence agencies, released '10 Steps to Cyber Security' to directly target the most senior levels in the UK's largest companies to provide them with advice on how to safeguard their most valuable assets, such as personal data, online services and intellectual property.

In Iain's Foreword he claimed that few companies have an appropriate cyber security governance regime, suggesting that, where this is the case, *'your IT systems may have already been compromised, attackers could already have your new product plans, bidding positions or research'*.

The document cautions that organisations must *'Put Cyber Security On The Agenda Before It Becomes The Agenda'*. It very much focuses on Governance, claiming that the Board has *'Ultimate responsibility for cyber security'*. It advises organisation to seek assurance that key information risks are both assessed and prioritised.

Iain claimed that *'a tangible difference'* can be made to the vulnerability from cyber attacks where companies adopt these *'basic information security practices'* (steps). A summary of the steps is as follows:

- **Information Risk Management Regime:** A call for Governance and for Boards to position cyber risks on the agenda with all other business risks. This step features as the overarching principle for all the following controls; each control must be activated firstly by policy.
- **Home & Mobile Working:** For which policies and training are required; protecting data in transit (meaning over a network or on a portable device) and at rest (device encryption).
- **User Education & Awareness:** Producing user security policies and procedures and ensuring sufficient training is in place for user awareness of the cyber risks.
- **Incident Management:** Establish and test incident response and disaster recovery capabilities.
- **Managing User Privileges:** Limit user privileges & monitor user activity.
- **Removable Media Controls:** Produce a policy to control all access to removable media. Limit media types & use.
- **Monitoring:** Establish a monitoring strategy & produce supporting policies.
- **Secure Configuration:** Apply security patches & ensure that the secure baseline configuration of all ICT systems is maintained.
- **Malware Protection:** Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.
- **Network Security:** Protect your networks against external and internal attack.

Progress on the UK Cyber Security Strategy – December 2012 [7]

In December 2012 The Rt Hon Francis Maude released the second Written Ministerial Statement detailing the Progress on the UK Cyber Security Strategy. The Statement alludes to a press article proclaiming the UK, as of 2012, to be the *'the most internet-based economy'* and a further study, which claimed that threats to our cyberspace had increased concurrently with the growth of the internet economy. The Minister referred to a recent PWC survey, which found that *'93% of large corporations and 76% of small businesses had a cyber security breach in the past year. With the cost for a security breach estimated between £110,000-250,000 for large businesses and £15,000-30,000 for smaller ones'*. The Minister commented also that *'Attacks on government departments continue to increase.'*

In response to the Cyber Security Strategy, the Minister claimed developments or improvements in

new or ongoing strategies in which government departments and agencies have been involved. The Minister also claimed that government-industry, and industry-industry collaboration had taken place with positive outcome, but mainly in industry-industry partnerships.

The Minister claimed a host of strategic goals since the release of the NCSP, but the following are some of the reported tangible returns:

- The **Police e-Crime Unit** had a return on investment of £72 harm averted for every pound invested by the NCSP. This was apparently based on a four-year plan, but the values reported had been delivered within the first year.
- **SOCA** has repatriated over 2.3 million items of compromised data to the financial sector in the UK and internationally since November 2011 with an estimated prevention of potential economic loss of over £500 million.
- The **Crown Prosecution Service** (CPS), as at the end of September 2012, was prosecuting 29 live cyber crime cases.
- NCSP funding has enhanced **Action Fraud** to be the UK's national reporting centre for fraud and financial internet crime, operating on a 24/7 basis. Over 12 months, Action Fraud received 46,000 reports from the public of cyber-enabled crimes amounting to attempted levels of fraud of £292 million.
- HMRC's enhanced anti phishing capabilities are now leading to the interception of five major threats a day and have helped shut down almost 1000 fraudulent web sites in the last 12 months.
- In April 2012, SOCA led a global day of action to tackle Automated Vending Cart websites selling compromised financial data. Two arrests were made in the UK and 70 websites taken down world-wide.

Future Cyber Plans

The national approach to cyber incident management is under review and there is an intention to move towards the establishment of a UK National CERT (Computer Emergency Response Team).

CESG and CPNI also recently launched a new scheme to help organisations respond effectively to the consequences of cyber security attacks. This is a HMG quality-assured service. **Regency IT Consulting** is one of the first organisations to support this scheme through their parent company Cassidian, a member of the EADS Group.

Development of a permanent information sharing environment called Cyber-security Information Sharing Partnership (CISP) is to be launched in January 2013. CISP will be initially open to companies within Critical National Infrastructure (CNI) sectors, but the intention is to make membership available more broadly, including to SMEs, in a second phase.

Also as a future initiative, funding has been earmarked to support the Institution of Engineering and Technology (IET) to open the Trustworthy Software Initiative, which aims to improve cyber security by making software more secure, dependable and reliable.

From spring 2013 the Cabinet Office will be rolling out a programme of public awareness drives. The programme will be delivered in partnership with the private sector and will aim at increasing cyber confidence and measurably improving the online safety of consumers and SMEs.

An example of government mainstreaming cyber security measures is HMRC automatically alerting customers using out of date browsers and directing them to advice on the threat this might pose to their online security.

Regency IT Consulting's View

The government is moving apace with new strategies and it is terrific news that it considers cyber security as one of its top priorities. It has set a structure for improvement in this area, but has a long way to go. The truth is, whilst threat actors pointed out in the Cyber Security Strategy of 2011 (*'organised criminals, terrorists, hostile states, and 'hacktivists''*) prevail unchecked, the cyber issue will remain. Furthermore, and as highlighted in the December 2012 Progress Statement, whilst internet-based business continues to rise, so will internet-based crime. The virulence of these attacks is rising faster than the capability of our defences, and the gap is increasing. The battle for absolute Information Assurance will, without doubt, be long and drawn out.

Evolving technologies combined with the cyber threats, people's desire to conduct everyday personal and business functions with these evolving technologies, and the vulnerabilities brought about by manoeuvring into an unproven security environment, is only ever likely to bring about risks to business areas that allow their use. With the vulnerabilities brought about by the

interconnectivity of industry-industry, government-industry, and multi-national partnerships declared as necessary by the Cyber Security Strategy itself, the knock-on effect is inevitably going to bring about sector-to-sector- and internationally-sized risks that we will need to find ways and means to mitigate.

Experience has shown that the biggest mistakes made by risk managers in both public and private sectors is not including a quantitative element alongside an otherwise qualitative approach to risk management, in other words what would be the actual financial cost of the loss or temporary absence of a particular information asset and how much would it cost to fix or replace. Rationale should only be applied once the figures are in, thereby combining the quantitative and qualitative thought process.

How Regency Can Support Your Information Risk Management

Regency has a team of very experienced consultants that specialise in information risk management in both public and private sectors. Our consultants working within your organisation will establish or improve an information risk management regime in order to meet your business requirements.

Where necessary, Regency ITC can employ a fully automated information risk management tool, CiticusOne, to assess an organisation's extant security controls against compliance with the relevant standards (SPF, PIA, IAMM, ISO27001, Sarbanes-Oxley, CoBit, SCADA, etc). Other standards bespoke to an individual business area can also be conducted.

The use of Citicus will not only reduce the time it will take to carry out the information risk management process, the time utilised by security practitioners and consultants, but will also reduce the costs of maintaining a real-time effective information risk management regime that once adopted can be updated on demand when the threats, vulnerabilities, scope, etc, change.

As the sole UK-based implementation partner, Regency can host and manage CiticusOne in our HMG accredited secure data centre and also provide the expertise to carry out independent evaluations. We can also arrange the training for personnel to use the software to maintain and update their risks and actions by using our hosting service via secure HMG VPN encrypted connections.

References:

[1] National Security Strategy 2010: http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf

[2] The Strategic Defence and Security Review 2010: http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf

[3] NATO Lisbon Summit 2010: http://www.nato.int/cps/en/natolive/official_texts_68580.htm

[4] Cybersecurity Summit 2010: http://www.scmagazineuk.com/risk-management-and-compliance--is-it-finally-all-coming-together/article/208453/

[5] Cyber Security Strategy 2011: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

[6] '10 Steps to Cyber Security': http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive

[7] Progress on UK Cyber Security Strategy 2012: http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_Cyber_Strategy_3-Dec-12_3.pdf