pitmans
MAKING IT HUMANLY POSSIBLE

Cyberspace – Industry and the Cyber Armoury

In this, the second in Pitmans' industry briefing papers following on from A Call to Economic Arms (http://bit.ly/e4ALOJ), we examine the issues posed by the emergence of Cyberspace as an increasing threat to national security, business activity and personal property. The largely positive transformation in the delivery of public services, commercial activity and personal communications enabled by the internet has however been mirrored by the emergence of cyber attacks on nation states' critical national services and infrastructure; attacks on business to defraud and steal intellectual property and criminal activity targeted at individual users. The threat from Cyberspace is now acknowledged by Government as one of the UK's top four risks identified within the National Security Strategy. What action is the UK Government taking? How can industry assist Government to protect our public services and critical infrastructure? What effective measures can business take to safeguard itself and its employees against the threats?

Introduction

There has been much exposure given to the cyberspace domain recently in the news and press. It attracts extensive attention from the Government, at all levels. The Foreign Secretary, William Hague, in his recent speech to the Munich Security Conference[1] noted both the geo-political threats from cyberspace as a '*new means of repression, enabling undemocratic governments to violate the human rights of their citizens'* as well as the staggering threat to businesses and individuals from cyber crime - '*over 40,000 pieces of sensitive information and financial data are traded on the online black market every day, amounting to 13.2 million criminal transactions every year'.*

Many commentators consider that references to 'cyber- warfare', apocalyptic scenarios of the shutdown of national infrastructures and conflicts fought purely in cyberspace are unrealistic hyperbole. Regardless of the semantics, cyberspace is unavoidably relevant to the private sector and the way businesses manage risk.

The reasons are primarily twofold: Firstly, any business which uses networked computers is potentially exposed to external cyber-threats, whether maliciously directed to it or not. Secondly, the threat can be internal in the form of innocent use of IT by employees which unwittingly exposes the business to significant corporate risk. Prudent businesses should recognise the magnitude of the cyber threat, assess its potential impact(s) on both their operations and business critical information and deliberately implement a safe and resilient cyber security capability as part of their formal policies on:

(i) Information management including with 3rd parties and suppliers etc.
(ii) Business continuity and contingency planning;
(iii) Corporate governance and reputational management;
(iv) Employees' use of company IT and other connected devices.

As part of a company's approach to managing the risks relating to (i), (ii) and (iii) above, employee training on the nature of cyber-threats, clear policies on the use of IT for non-work purposes and standard operating procedures for reporting suspect activity should become the norm. Any culture of complacency about cyber security increasingly runs significant risks which could be catastrophic for a business's ability to trade as well as its reputation. It is difficult to mitigate the scenario of encountering a deliberate attack on IT systems from someone inside the business – akin to the 'Insider Threat'. However, as Andrew Peddie, Pitmans Head of Corporate noted in his article, UK Businesses and the Cyber Threat of 2 November 2010 (http://bit.ly/9FWufk).

[1] William Hague in his speech to the Munich Security Conference, 'Security and freedom in the cyber age - seeking the rules of the road' 4 February 2011.

'We may find that [as a result of managing corporate risks] corporate life becomes less accommodating for employees in terms of free and easy access to external connectivity over time'.

At its extreme, the spectre of 'Botnet' armies created by criminals and anti Western States harnessing the power of thousands of personal and corporate computers with rogue software in order to attack systems and infrastructure is, we are reminded, not mere fantasy.[2]

Many readers of this paper will already be thinking of and/or actively dealing with these concerns and issues. It is not all negative. It is probably true to say that for the vast majority of businesses the benefits of cyberspace have far outweighed the negative experiences – but events such as the 2010 cyber-attack on Mastercard and Visa's systems leave no room for complacency. Given the rapid development of technology and the sophistication of those intent on harming the UK and its economic interests, it can be taken as a certainty that new threats will continue to arise.

Government and the cyber response

There is Governmental recognition of the strategic realities presented by cyberspace. This is demonstrated by the prominence given to cyber security with the creation of the Office of Cyber Security (OCS), the Cyber Security Operational Centre (CSOC) and the £650m funding for National Cyber Programme (NCSP) shortly to commence. This should be a signal flag to industry because the Government also recognises that it must engage industry in order to be able to meet its capability requirements and fulfil its duty of security to the nation. With this strategic need comes opportunity, particularly for those businesses operating in the IT domain.

The Opportunity Challenge for Industry/Business

The Government's Green Paper on Equipment, Support and Technology for UK Defence and Security published in December 2010 expressly states that the Government will '*seek to involve…private sector partners in a new joint programme of activity'*.[3] For the UK's cyber security to be effective, the Government has to work hand in glove with private sector – cyberspace cannot be compartmentalised neatly into public sector and private sector cyber environments. The encouraging statements of intent in the Green Paper for developing joint initiatives and partnerships with industry to meet *'the challenges of cyber security'*[4] should be acknowledged.

However, it is less certain whether Government engagement with industry will become normative at the earliest stages of research, trials and development in the production of the UK cyber armoury. Historically, as is well documented, procurement processes have been a bar to smaller industry players directly engaging with Government with the result that the identified capability requirements have often been out of sync (from the moment they are defined) with the technology available in the wider market place. It remains to be seen how the Defence Acquisition Reform Programme (DARP) alters this landscape. There can be no room for such a disconnect in an environment which changes rapidly, appeals to innovative technology and where the risks of being behind the pace are so significant.

Further, business should be wary of adopting a perception that it will be able to follow where the Government leads, notwithstanding the importance the Government has assigned to cyber security. In comparing the UK private sector annual spend on ICT of circa $187 billion (dollars cited) with the Government spend of c. £16 billion, the UK technology trade body, Intellect, contends 'that it is commercial interests that drive the cyber agenda'[5]

There are indeed some particular aspects of the UK's capability requirement in cyber security which point to a specific UK industry centric approach. The Green Paper recognises the importance of maintaining sovereign capability over strategically crucial aspects of cyberspace such as the production and management of cryptographic material. UK companies may also

[2] As indicated in BBC Newsnight, 10 February 2011 in its piece on Cybersecurity and the example of such activity emanating from Estonia.
[3] Paragraph 214 of The Green Paper.
[4] Paragraph 218 of The Green Paper
[5] As cited on page 6 of Intellect's Paper, Improving Cyber Security Partnerships, November 2010

consider whether they can offer a security advantage in the supply chain in producing software and technology which, if produced abroad, may be more susceptible to malicious components being placed within it.

Back to the company's own doorstep

As identified in the first section of the article, companies - particularly those where knowledge assets are key, e.g. finance, pharmaceuticals, engineering - should make it a priority to ensure that formal risk management is also directed to the risks posed to corporate integrity by cyberspace.

Practical considerations for companies include the following:

- Actively identify risks and vulnerabilities to the business from the cyber domain, assess the potential impacts on both its own commercial integrity and that of its customer/suppliers and implement protection and risk mitigation. Pitmans' advice to those responsible for dealing with these particular risks is aligned with understanding these cyber risk drivers in order to assist companies to remain profitable, discharge their duties to shareholders and comply with statutory or other requirements under which a company is bound.

- Define and mandate policies for the use of company IT by employees and staff for non work applications including Facebook, Twitter and other social networking media. Pitmans employment lawyers advise on these policies and are giving a free seminar **'Watching from the Sidelines – social media and employee monitoring'** on **13th October 2011** in Reading (http://bit.ly/g84zoa).

- Ensure that minimum IT security standards and company policy on use of IT is, where necessary and possible, contractually reflected in T&Cs with contractors, suppliers or others connected with the business. Pitmans commercial and technology sector lawyers advise on such measures.

- Those companies involved in acquisitive activity in the international technology/IT scene – particularly where the target company's country or base is more susceptible to interference by those who may seek to harm the UK's interests – should consider the need for due diligence on the provenance of the target company's technology/products. Pitmans commercial and technology lawyers advise on these particular considerations.

The cyberspace domain is one where managing risk in order to benefit from the reward of the opportunity it affords is crucial. The Government recognises its importance and we await the publication of the White Paper on Equipment, Support and Technology for Defence and Security due in April 2011 to see how industry's role is clarified in grappling with the imperatives it raises.

Pitmans will in the meantime be producing a further briefing paper on another key theme for industry advanced in The Green Paper – the Government's emphasis on **Exports.**

Jonathan Durrant
Director
T: +44 (0)118 957 0270
E: jdurrant@pitmans.com
www.pitmans.com/defence-security