
Executive Summary

Cyber Security and the UK's Critical National Infrastructure

Paul Cornish, David Livingstone, Dave Clemente
and Claire Yorke

A Chatham House Report

Read more

www.chathamhouse.org/cyber_cni



CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE

T: +44 (0)20 7957 5700 E: contact@chathamhouse.org

F: +44 (0)20 7957 5710 www.chathamhouse.org

Charity Registration Number: 208223

Executive Summary and Recommendations

Dependence on information and communications technology (ICT) is a defining feature of a modern, interconnected and knowledge-based society and economy. The machinery of government, critical national infrastructure (CNI) – including the provision of essential services such as water, gas, electricity, communications and banking – and much of the straightforward private life of individual people are all ICT-dependent to a large degree. With this dependency can come vulnerability to aggressors, criminals and even the merely mischievous.

Public and media attention is frequently drawn to tales of hacking and espionage and there is persistent concern about the rapid growth of cyber crime such as banking fraud and identity theft. The discovery of the Stuxnet virus in 2010 provided evidence of the growing sophistication of cyber threats and the potential damage they could cause to governments, organizations and critical infrastructure around the world.

It is clear both that the sense of threat and vulnerability is mounting and that the public and private sectors are under increasing pressure to ‘do something’ about cyber security. The United Kingdom National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) released in October 2010 promoted cyber security to a Tier One risk to national security, and its high status was reinforced by the UK government’s allocation of £650 million to cyber security and resilience.

What should be done to meet this challenge? And who or what is best placed to tackle the problem, given that

£650 million will hardly enable the government to counter all conceivable cyber threats and that, in any case, the vast majority of critical infrastructure in the UK is privately owned?

Cyber stakeholders

The first task should be to identify all those with a stake in cyber security, as the essential basis for the development of a national culture of cyber security. Yet there is currently no publicly available, comprehensive account of the UK national cyberspace stakeholder environment that could provide the basis for the development of a national cyber security regime, culture or policy framework. This report aims to fill that gap.

The Centre for the Protection of Critical National Infrastructure and the UK *Cyber Security Strategy* include in their definition of critical national infrastructure (CNI) communications, emergency services, energy, finance, food, government and public services, health, transport and water. Taking this definition as its starting point, this report asks whether the various agencies, bodies and individuals involved recognize the significance of the cyber stakeholder status that has been conferred upon them. How do these organizations identify and measure their cyber dependencies, and how well and systematically do they manage the risks and mitigate the potential vulnerabilities associated with these dependencies?

The report is based on a series of high-level interviews through which the authors sought to gauge the various organizations’ overall understanding of, and response to, the problem of cyber security. Rather than interview communications officers or representatives of IT departments, the authors sought wherever possible to assess the level of cyber security awareness at board level, and particularly among the most senior executives who had no specific IT expertise.

Threat perceptions

With regard to threat perceptions and sensitivity, the principal finding of the report is that there appears to be no coherent picture or sense of what constitutes a vulnerability, or of the likely severity of the consequences of

that vulnerability. There is, in short, no agreement on the nature and gravity of the problem that is either so compelling or so widely accepted as to catalyse a society-wide response to the challenges of cyber security, embracing the public and private sectors.

Many interviewees shared the perception that the national response mechanism is for the most part fractured and incoherent. There are many sources of information on cyber threats, including specialist media and government briefings and alerts from security software companies. Yet there appears to be widespread dissatisfaction across the CNI with the quality and quantity of information-sharing between the public and private sectors. There was considered to be an absence of an authoritative 'rich picture' generated at the centre (i.e. by government) that could help to develop a more comprehensive and urgent sense of the cyber threats that need to be tackled. This picture would improve the awareness of risk in and from cyberspace and would enable a more effective collective response. The richness of this threat picture is dependent upon the willingness to share sensitive information, and to do so in a timely manner. However, the UK government is perceived by many, whether justifiably or not, to be more willing to solicit information than to divulge it.

The 2010 NSS and SDSR both stress the importance of cyberspace to national security. There is as yet, however, little sense either of governmental vision and leadership, or of responsibility and engagement within the CNI that could encourage a well-informed and dynamic political debate on cyber security as a national challenge.

Yet government cannot provide all the answers and cannot guarantee national cyber security in all respects and for all stakeholders. As a result, the report concludes that CNI enterprises should seek to take on greater responsibility and instil greater awareness about the nature of cyber risks across their organizations. Senior management should, for example, create incentives for departments and individual employees to recognize and address cyber dependencies and vulnerabilities as they arise. However, this will only be achieved to the extent that board members are themselves more aware of the opportunities and threats presented by cyberspace.

Organizational approaches

Many of the organizations surveyed in the course of this project have developed an attitude to cyber security that is fundamentally contradictory. In most cases, they declared themselves to be aware of cyber security threats. Yet these same organizations were willing, for a variety of resource and other reasons, to accept an unexpectedly high level of risk in this area. In several cases it was even decided that cyber risk should be managed at arm's length from the executive authority and responsibility of the board and senior management. Paradoxically, therefore, in these organizations a heightened perception of cyber security risk is being met with diminished resources and interest.

Several senior executives expressed a wish to become more intelligent customers, feeling that at present they speak a different language from their ICT professionals and are thus unable to consider cyber security issues in sufficient depth. It appears that more fundamental behavioural transformation is required, with the needs of the business driving ICT security rather than the other way around. This in turn requires IT security departments to develop a deeper understanding of how value is created in the organizations they endeavour to protect. For their part, the senior managers of organizations, both large and small, can no longer afford to treat cyber security as the remit of only one department. The potential for damage, both economic and reputational, from complacency over matters of cyber dependency and vulnerability is too high to be ignored by even the largest multinationals.

Although the report identified shortcomings in the management of the cyber security response in the CNI, more encouraging practices were also found. However, such incidents of 'best practice' were scattered haphazardly across the range of organizations interviewed. Most strikingly, the quality of practice could vary significantly within an organization, with some displaying both the 'best' and the 'worst' practices and behaviour in their sector. A simple expedient to raise the general level of awareness of good cyber security practice across the CNI and, by extension, across society more broadly, would be to develop a single, accessible bank of cyber security information and advice upon which organizations, enterprises, government bodies and individuals could draw.

Key recommendations

The cyber security threat cannot be met by government alone. The potential for cyber attacks to cause damage at a societal level calls for a coordinated response in which dependencies and vulnerabilities in infrastructure, industry and key organizations can all be identified and addressed. Given the scale and scope of the challenge, responsibility for the solution should be shared by government and the CNI. Acknowledging this imperative, what follows is a series of policy recommendations intended to drive a collaborative effort between the private and the public sectors.

Perceptions and the threat landscape

1. Although there is growing awareness of the threats and risks in cyberspace, there is still limited understanding of the nuances of the debate. The government should assume an integral role in shaping the discourse, informing wider society and raising levels of awareness. Government can act as a focal point for collating information while creating a broad picture in partnership with the private sector.
2. Government and the wider CNI should recognize and respond to the rapid pace of change in cyberspace and to the heterogeneous nature of cyber threats through more comprehensive internal strategies and risk awareness levels as well as updated and dynamic technologies and management processes.
3. Organizations should look in more depth at dependencies and vulnerabilities that may be hidden in other organizations on which they are dependent and which are part of a common supply chain.
4. There is a need for organizations to acknowledge and respond to the potential damage that organizational insiders can cause without interfering in the levels of productivity and creativity.
5. Research and investment in cyber security are essential to meeting and responding to the threat in a timely fashion and to nurturing human resource capabilities yet this area is currently under-resourced and lacks the appropriate long-term funding in both the public and private sector.

Managing cyber dependencies

1. Cyber security should be a fundamental component of an organization's risk strategy. While there will inevitably be 'unknown unknowns', more thorough risk assessments and more agile response mechanisms will narrow the chances of strategic shock and will increase overall resilience against cyber threats.
2. There is a need to address organizational inconsistencies in risk management and to develop a more comprehensive understanding of risk as it relates to cyber security.
3. Senior management will need to be more aware of the range of cyber dependencies within their organization and the budgetary and reputational implications of vulnerabilities. They should be sufficiently confident to ask the right questions from those tasked with providing security within their organization.
4. In the pursuit of efficiency savings and improved quarterly returns, companies should take care not to undermine risk mitigation strategies and contingency planning. Clear plans are needed and adequate resources must be allocated for disaster recovery.
5. CNI organizations will need to look further ahead to identify potential threats and to develop anticipatory responses to the potential cyber risks within the organization.
6. Training and development of staff in cyber security measures should be seen as an integral part of risk mitigation strategies.
7. The management of cyber dependencies will require the cooperation of CNI and government, and an effective collaboration should seek to clarify responsibilities and expectations within both the public and private sectors and at the correct designated level of responsibility.

Information communication and outreach

1. Detailed, specific information communication and outreach strategies are essential to achieving consistency in managing cyber risks as part of a systematic approach to developing a culture of awareness. These should be targeted at, and tailored for, both board-level members and technology experts and disseminated across organizations to enhance overall awareness of the issue.

2. Internal strategic communications regarding cyber threats should be transmitted across an organization with a clear sense of decision-making hierarchies (or 'chains of command'), responsibility and accountability.
3. Government will have to communicate with senior private-sector management in language the latter can understand. The issue of cyber risks needs to be made accessible for those who are neither familiar with technology nor highly IT-literate.
4. Cyber terminology should be clear and the language proportionate to the threat. It should also encourage a clear distinction to be made between IT mishaps and genuine cyber attacks.
5. As part of communication and outreach efforts it would be useful to have a centre of intelligence-sharing such as the Virtual Task Force (which is used to coordinate approaches to cyber crime among financial institutions) for those who need to be informed so that decisions can then be made and information disseminated both vertically and horizontally between affected organizations.
6. Greater public awareness would help acclimatize a wide audience to cyber security issues and encourage individual precautions and security measures. Public messaging must recognize the existence of disparities and varying levels of awareness.

Building a cyber security culture

1. Greater organizational and public awareness is essential to inform and shape an effective national cyber security culture.
2. Examples exist of best practice but these need to be standardized across the private and public sectors. Government and industry will need to work together to develop accepted models of best practice as well as common terminological standards.
3. Incorporating cyber risk into existing risk cultures will mean considering it together with wider organizational risks. It needs to be a standard item on the agenda rather than being seen as distinct, inscrutably complex and 'someone else's problem'.
4. A robust cyber security culture should be responsive to the rapid pace of change in technology and innovation.
5. Providing commercial and professional incentives for the private sector and broader society could positively stimulate and shape a national cyber security culture and motivate better practice, but this will require more effective communication and outreach strategies which simultaneously convey the nature of the problem and appropriate responses and precautions in a way that is accessible to a diverse array of organizations and individuals.