Global Cyber Security Capacity Centre

Cybersecurity Capacity Review of the United Kingdom

Global Cyber Security Capacity Centre
University of Oxford
November 2016

About the Global Cybersecurity Capacity Centre

The Global Cyber Security Capacity Centre (GCSCC) is a leading international centre for research on efficient and effective cybersecurity capacity-building, promoting an increase in the scale, pace, quality and impact of cybersecurity capacity-building initiatives across the world.

Lead Editor and Author

Dr Maria Bada

Authors (listed alphabetically)

Professor Ivan Arreguín-Toft
Professor Ian Brown
Professor Paul Cornish
Professor Sadie Creese
Professor William Dutton
Professor Michael Goldsmith
Ms Eva Ignatuschtschenko
Ms Lara Pace
Ms Lilly Pijnenburg Muller
Mr Taylor Roberts
Professor Sebastiaan Von Solms
Professor David Upton

Acknowledgments

Special thanks to Dr Jassim Happa for his assistance on the creation of the visualisation of the cybersecurity capacity maturity model in use across all reports.

Contact details

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk
Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Contents

Abbreviation List 4

Introduction 5

Executive Summary 7

Review of Cybersecurity Maturity 16

Dimension 1: Cybersecurity Policy and Strategy 18
- D1-1: Documented or Official National Cybersecurity Strategy 18
- D1–2: Incident Response 19
- D1-3: Critical National Infrastructure (CNI) Protection 21
- D1-4: Crisis Management 22
- D1-5: Cyber Defence Consideration 23
- D1-6: Digital Redundancy 25
- Recommendations 25

Dimension 2: Cyber Culture and Society 28
- D2-1: Cybersecurity Mind-set 28
- D2–2: Cybersecurity Awareness 30
- D2-3: Confidence and Trust on the Internet 31
- D2-4: Privacy Online 32
- Recommendations 34

Dimension 3: Cybersecurity Education, Training and Skills 36
- D3-1: National Availability of Cybersecurity Education and Training 36
- D3–2: National Development of Cybersecurity Education 38
- D3-3: Training and Educational Initiatives within the Public and Private Sector 39
- D3-4: Corporate Governance, Knowledge and Standards 40
- Recommendations 41

Dimension 4: Legal and Regulatory Frameworks 44
- D4-1: Cybersecurity Legal Frameworks 44
- D4–2: Legal Investigation 47
- D4-3: Responsible Reporting 48
- Recommendations 49

Dimension 5: Standards, organisations, and technologies 51
- D5-1: Adherence to Standards 51
- D5–2: National Infrastructure Resilience 53
- D5-3: Cybersecurity Marketplace 54
- Recommendations 55

Appendix I 58

Appendix II 69

Abbreviation List

ACEs-CSR Academic Centres of Excellence in Cyber Security Research
BIS Business Innovation and Skills
CBEST Central Bank Ethical Security Testers
CCPs CESG Certified Professional
CESG Communications-Electronics Security Group (National Technical Authority for Information Assurance)
CISM Certified Information Security Manager
CiSP Cybersecurity Information Sharing Partnership
CISSP Certified Information Systems Security Professional
CLAS CESG Listed Advisor scheme
CMORG Cross Market Operational Resilience Group
CNI Critical National Infrastructure
COBR Cabinet Office Briefing Room
CPNI Centre for the Protection of Critical Infrastructure
CPS Crown Prosecution Service
CREST Council of Registered Ethical Security Testers
CSIA Cabinet Office Central Sponsor for Information Assurance
DHCSTC Defence Human Capability Science and Technology Centre
EPSRC Engineering and Physical Sciences Research Council
ICO Information Commissioner's Office
IOCCO Interception of Communications Commissioner's Office
ISO International Organisation for Standardisation
IETF Internet Engineering Taskforce
3GPP 3rd Generation Partnership Project
GSCF Gloucestershire Safer Cyber Forum
GCHQ Government Communications Headquarters
KPIs Key Performance Indicators
LGD Leading Government Departments
NCA National Crime Agency
NCCU National Cyber Crime Unit
NCSP National Cyber Security Programme
OCS Office of Cyber Security
NSS National Security Strategy
SANS System Administration, Networking, and Security Institute
SDSR Strategic Defence and Security Review
SMEs Small and medium-sized enterprises
SOCs Security operations centres
TISAC Telecommunications Industry Security Advisory Council

Cybersecurity Capacity Review of the United Kingdom

Introduction

At the invitation of the government of the United Kingdom, the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity in the UK, supported by the host team (Office of Cyber Security and Information Assurance within the Cabinet Office – OCSIA). The objective of this review is to enable the UK to determine areas of capacity in which the government might strategically invest in order to become more cyber secure. The GCSCC review will contribute to the development of the UK National Cybersecurity Strategy 2016–2020.

During September (16th, 17th, 18th) and October (2nd) 2015, stakeholders from the following sectors participated in a four-day consultation to review cybersecurity capacity in the United Kingdom:

- Government Departments and Ministries: Ministry for Culture, Communications and Creative Industries; Security and Justice Team; Department for International Development; Department for Business, Innovation and Skills; Association of Chief Police Officers (ACPO); National Fraud Authority; The Office for Security and Counter -Terrorism (OSCT) of the Home Office; Ofcom (Independent regulator and competition authority for the UK communications industries); Conflict Humanitarian and Security Department; Finance and Corporate Services – ICT Business Strategy & Planning; National CERT-UK.
- Academia
- Criminal Justice and Law Enforcement
- Legislators/Policy owners
- CERT and IT Leaders from Government and the Private Sector
- Private Sector
- Telecommunications companies
- Finance sector
- Cyber Task Force

We conducted eleven sessions to review cybersecurity capacity in the United Kingdom, hosted in the offices of the Cabinet Office and the Foreign and Commonwealth Office (FCO). It has to be noted that a broader participation from all sectors would have been preferred in order to capture different views and perspectives on cybersecurity capacity in the UK, within central and local government, the private sector and wider society. The Roundtable discussions were followed by the distribution of a survey format of the Cybersecurity Capacity Maturity Model (CMM)[1] to a wide range of stakeholders (30 stakeholders were contacted).

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model which is composed of five distinct areas of cybersecurity capacity, a) policy and strategy; b) culture and society; c) education, training and skills; d) legal and regulatory frameworks; e) standards, organisations, and technologies.

[1] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

There are multiple factors in each dimension, which describe what it means to possess cybersecurity capacity. In each factor, there are indicators spanning, five stages of maturity, whereby the lowest stage implies a rather ad-hoc level of capacity and the highest stage both a strategic approach and an ability to dynamically adapt or change against environmental considerations. The five stages are as follows:

- **Start-up:** At this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence at this stage.
- **Formative:** Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the sub-factor are in place, and working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the "relative" investment in the various elements of the sub-factor. But the indicator is functional and defined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important for the particular organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional upon the nation or organization's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technology of the threat environment, global conflict or a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this stage.

Following the cybersecurity capacity review of the United Kingdom, results are being displayed in the present report, including recommendations on the next steps to be taken into consideration by the Her Majesty's Government (HMG).

Cybersecurity Capacity Review of the United Kingdom

Executive Summary

The Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') has facilitated a review of the cybersecurity capacity of the United Kingdom, hosted by the Office of Cyber Security and Information Assurance within the Cabinet Office (OCSIA). The objective of this review is to enable the United Kingdom to determine the areas of capacity that the country might strategically invest in to enhance its cybersecurity resilience.

During September (16th, 17th, 18th) and October (2nd) 2015, stakeholders from the following sectors participated in a four-day consultation to review cybersecurity capacity in the United Kingdom: Government departments and ministries, academia, criminal justice and law enforcement, legislators and policy owners, CERT and IT Leaders from Government and the private sector, major industry and SMEs, telecommunication companies and the financial sector. The consultations were premised on the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five distinct dimensions of cybersecurity capacity:

- Cybersecurity policy and strategy
- Cybersecurity culture and society
- Cybersecurity education, training and skills
- Cybersecurity legal and regulatory frameworks
- Cybersecurity standards, business models and technologies

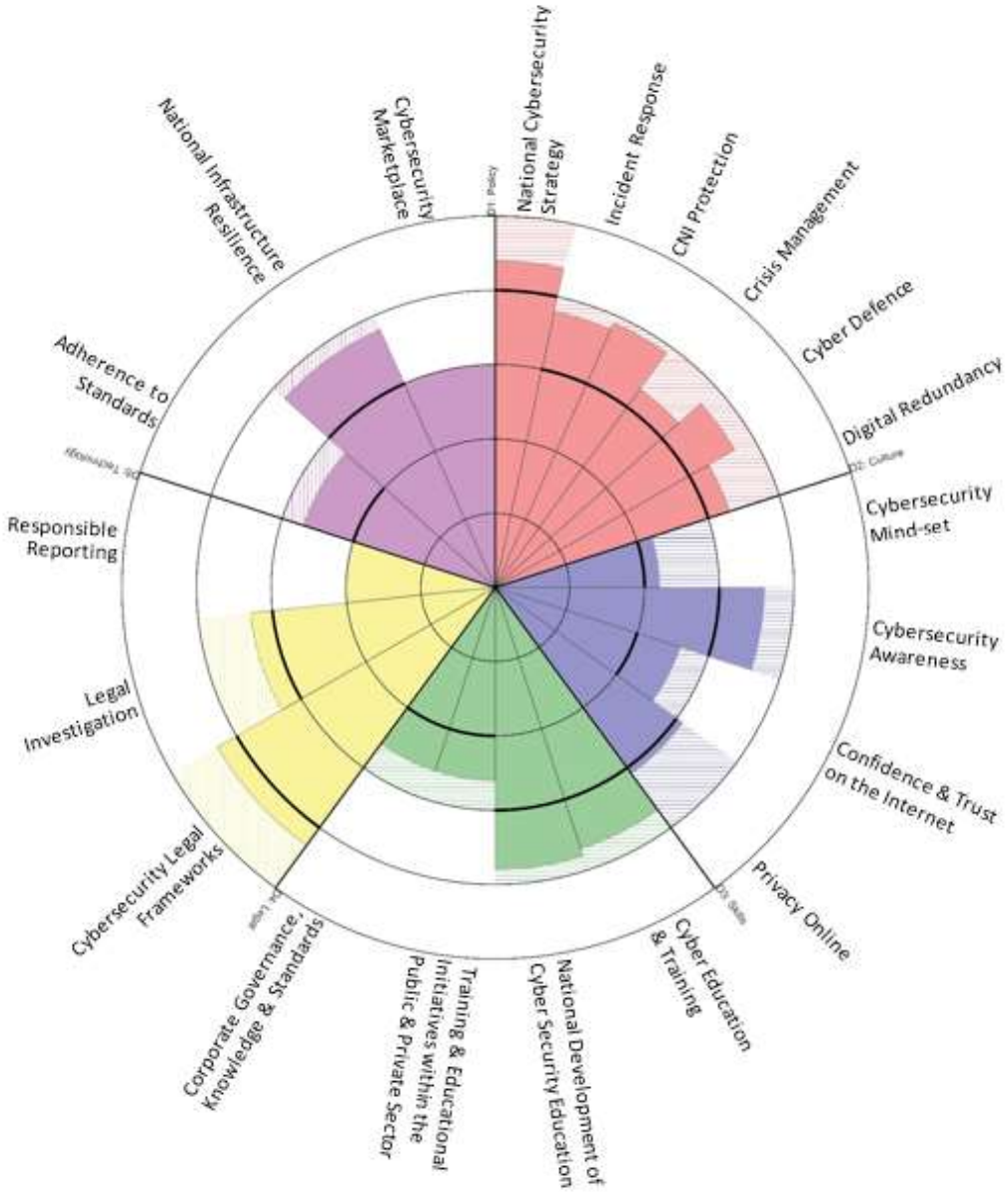
Based on the evidence collected across the five dimensions, for the majority of the factors considered within the Cybersecurity Capacity Maturity Model (CMM), cybersecurity capacity in the UK lies between an *established* and *strategic* stage of maturity. However, for certain factors in Dimension 1 (Strategy and Policy) and in Dimension 4 (Legal and Regulatory Frameworks), maturity seems to be at a higher (*dynamic*) stage. Furthermore, as illustrated in Graphic I below, for a number of factors progress is already being made towards a higher stage of maturity. However, according to the methodology followed during the deployment of the Cybersecurity Maturity Model (CMM), the indicators for a certain stage need to be fully achieved for that stage of maturity to be assigned; maturity is recognised only at the highest completed stage. The assignment of maturity stages is based upon our interpretation of the evidence including the general or average view of accounts presented by stakeholders, desktop research conducted, and our professional judgement.

A total of eighty-four recommendations have been made, detailed in the main body of the report, as well as shown in Appendix II. What follows here is a summary of our findings and key resulting recommendations.

With regards to strategy, the government is now in the process of revising the National Cybersecurity Strategy (2015–2020), based on threats, lessons learned and outcomes of the existing strategy implementation. There is a regular annual review of the National Cyber Security Programme (NCSP). The National Security Strategy is implemented by multiple stakeholders across government but is only starting to take into account all levels that have to be considered, while translating the strategy to all governance levels (police forces, etc.). No mechanism is yet in place to implement the national cybersecurity strategy in its full scope, especially at a local level.

Graphic I: Review Results

Black highlighted borders in Graphic I indicate the end of a stage. It is a simple matter, therefore, to indicate where progress is already underway towards reaching the next stage of maturity in many indicators. Diagonal lines indicate the remaining areas of capacity required to reach the next stage of maturity for a particular factor.



For these reasons, stakeholders agreed that the development of the National and Cyber Security Strategies, although at a strategic stage of maturity, is not yet at a dynamic stage. In order to achieve more agility there is arguably a need for broader participation of stakeholders during the evaluation of the national cybersecurity strategy, including the private sector, wider society and international partners, which moves beyond this normal review process.

A broader conversation with all stakeholders including the private sector, civil society and international partners during the annual review of the National Cyber Security Programme (NCSP) is recommended.

Regular scenario and real-time cyber-exercises are conducted in the UK. A central registry of national-level cyber-incidents has been established and is held by CERT-UK, but there is no central responsibility for incident response, and no clear regulation to ensure that all incidents are reported (nor a regulatory regime to incentivise such). With respect to coordination, the responsibility for *incident response* has been allocated within each public administration entity, governmental department and ministry. While the Cyber-security Information Sharing Partnership (CiSP) platform that CERT-UK supports is expected to help support information sharing between the public and private sector, this mechanism is still evolving and our understanding is that the nature of information being shared is variable, and the operational benefits also variable. More mechanisms for cooperation in this area are needed to enhance capacity, specifically with regard both to helping CNI organisations strengthen their security postures which may in turn strengthen the UK national security posture. In this respect, we recommend prioritising multi-level national coordination between all sectors for incident response including local and international level, drafting regulations on incident response and reporting, as well as the development of a defined mechanism for capturing incidents on lower governmental levels, locally.

While *Critical National Infrastructure* (CNI) assets have been identified, cybersecurity priorities and processes have not been synchronised well between the national and local levels. Defined reporting requirements between CNI asset owners and the public sector are perceived as sufficient to address national security needs; nevertheless, in our view this is not adequate to prevent significant harm manifesting from cyber-attacks. The reporting is necessarily limited to current ideas around good practice and therefore cannot promote the creative ideas around defence and incident response. Whilst the UK may be at the global forefront in implementing such practices, unfortunately, we (in the broadest sense) have a limited ability to accurately quantify a national security posture in a manner, which, for example, could consume such reporting and translate into stronger harm-prevention or risk-mitigation. Therefore, the UK cannot afford to be complacent in this area.

In terms of regulatory incident response, regulators cooperate with their respective ministries and agencies but cybersecurity incident response regulation is not always sufficiently adhered to, due to differing interpretations of required resilience. Therefore it is recommended to prioritise listing of CNI assets and regularly re-appraise to capture changes in the threat environment; implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio; strengthen formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector; execute procedures to optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations as needed.

While recognition of the importance of *crisis management* exercises is acknowledged, investment into such exercises, especially at a local level, remains insufficient possibly due to the difficulty in communicating the value of such exercises to stakeholders. Therefore, it is important to prioritise crisis management exercises, especially at a local level, and communicate the value of the exercises.

The evidence we collected suggests that while there is no dedicated, explicit, *Cyber Defence Strategy* or Doctrine in the UK, the Cyber Programme, the National Strategic Defence and Security Review and the National Security Strategy all function in tandem to achieve this purpose. We would expect the UK to be developing a defence strategy around cyber, and note that the UK is one of the countries leading the conversations in various international fora on cyber-defence. We suggest the draft of a Cyber Defence Strategy; review of the evolving threat landscape in cybersecurity to ensure that cyber-defence policies continue to meet national security objectives; prioritise compliance of the National Security Strategy and National Strategic Defence and Security Review with international law and consistency with national and international rules of engagement in cyberspace.

Regarding the *Cybersecurity Culture and Society* dimension, the review identified that capacity ranges from *formative* to *established* stages. There is a general lack of awareness regarding online risks and a safe behaviour online around the world and we expect that in every country there will be less maturity in this dimension. It was noted in our evidence collection that within the government the *cybersecurity mind-set* is typically reactive rather than proactive. At a governmental level, cybersecurity is a concern but there are differences among different departments at different levels of government, such as departments that have traditionally handled personal information, and those that have not. In particular, there is a lack of understanding of risks and threats at the local level. Agencies with a cybersecurity focus, such as CERT-UK and the Government Communications Headquarters (GCHQ), are considered the most adept and convincing at adopting a cybersecurity mind-set.

While the general public is becoming increasingly aware of cybersecurity threats, there is wide variation between individuals in their understanding of how to address these threats, and also in the routine practices of Internet users, with many not embedding even accepted good practice in their everyday use of the Internet. More needs to be done to raise the general skills and routines of Internet users in order to foster a higher level of maturity in this dimension. Whilst there is evidence of many initiatives, often involving or being led by industry, the evidence suggests that this is having limited impact across society, since these initiatives do not target all groups of society. Another issue raised was the gap between conceptions of cybersecurity between experts and other members of society, and how that difference might influence practices. Experts often have unrealistic expectations of the ordinary user. The case for harm resulting from a lack of national cybersecurity is not yet made to the general public. Therefore, there is a need to enhance efforts at all levels of government to promote understanding of risks and threats and promote prioritisation of risk and threat understanding for SMEs.

There are coordinated *awareness-raising* programmes in the UK and there is evidence of significant multi-stakeholder engagement in these efforts, especially in delivery of the awareness campaigns. However, these efforts do not necessarily cover all groups of society. There are awareness efforts, such as “Cyber Essentials”, a coordinated, government-backed, industry-supported scheme to help organisations protect themselves against common cyber-attacks. Programmes and materials have been made available to train and improve cybersecurity practices and there is a growing effort towards raising awareness in schools. Nevertheless, the majority of individuals in the UK are not well aware of the possible risks online and even increased awareness over time does not necessarily mean society is more

cyber secure. It was agreed that although awareness might exist, the appropriate by experts actions are not necessarily understood or taken. There are also metrics in place to assess the effectiveness of these programmes, and it is noted that the UK research community are world leaders in considering the effectiveness of metrics in these spaces. While these efforts are commendable, there is a perception that it is important for the private sector to provide awareness education, acknowledging the limitations on financial resources.

Concerning the private sector and its cybersecurity capacity risk management practices are being identified to counter growing cyber-threats. During the course of the review evidence suggested that larger companies prioritise cybersecurity related needs based on risk assessments, while SMEs are less accustomed to incorporating the management of cybersecurity risk into business practice. This was to be expected. Businesses in general are anxious about cybersecurity threats, but often are not sure of the actions they need to take. Although awareness may exist, appropriate actions are not necessarily taken. Evidence suggests that awareness of the threat amongst the leaders of the biggest businesses in the UK is high, possibly heightened due to the coverage in national media. However, this is not resulting in maturing of leaders' ability to contribute to the management of cyber-related risks in the boardroom; the perception is that this continues to be considered the problem of the technology or information officers. In our view this is likely to result in a lack of resources being dedicated to managing such risks, and over time this will manifest in successful attacks that could impact the security or prosperity of the country.

Regarding the enhancement of the existing capacity we recommend that the public sector maintain and expand the existing awareness programmes to cover various target groups linked to the national cybersecurity strategy; promote awareness of risks and threats at lower levels of the government and also encourage the private sector to provide awareness education.

The use of online services is increasing in the UK, especially by younger users, but there is not necessarily a corresponding increase in trust in the security of these services. It was noted by various stakeholders that people tend to *trust online services* regardless of secure service provision and this unsupported trust could be detrimental to cybersecurity efforts. Although some companies are making a significant effort to shift their services online, there is no coordinated programme on building trust in the security of these services. Furthermore, there is no coordinated programme to promote trust in e-government services. During our consultations it was suggested that local online services might be more trustworthy than those offered at the national level. A review of this nature is not mandated to investigate whether such views are well founded. However, whether UK organisations have access to the right technologies and standards to deliver trustworthy services is considered below. We recommend that the UK government consider improving the trustworthiness of both e-government services and online commercial services, while also addressing the general handling of private or personal data and develop a feedback mechanism to provide evidence on trust in e-government and e-commerce services. These measures should be undertaken alongside an effort to promote understanding of cyber-harm and cybersecurity, and of trustworthiness in services and technologies.

Debate and discussion around the handling of personal data by commerce and government, the positives and negatives to national and personal cybersecurity, and the personal risks to

individuals resulting from a lack of national or personal cybersecurity are not evidenced as being understood across society. This is likely to leave people, business and the country open to vulnerability and ultimately risk. During the consultation the perceived levels of understanding of privacy, both at the national and local levels of government, was a highly debated issue. Additionally, the data collected suggest that whilst there is clearly evidence of awareness of privacy standards and policies, this does not necessarily translate into day-to-day practice. *Privacy in the workplace* is recognised as an important component of cybersecurity and many employers maintain privacy policies that provide a minimum level of privacy for employees. Therefore, there is a need to promote the understanding and implementation of privacy standards and policies within the local government and private sector and sensitise employees on their privacy rights and obligations.

The review found the dimension concerning *Cybersecurity Education, Training and Skills* in the UK to be at an *established* stage. There are *educational offerings in cybersecurity* at national and local levels, ranging from primary to post-graduate. Many universities offer different types of cybersecurity courses, but only a few have an affiliation to industry. An issue raised during the review was that although there is a high amount of education available, it does not necessarily meet the needs of industry employers in terms of skills development, nor are educational offers measured to determine their success in meeting the skill needs of the job market. Stakeholders from the private sector expressed their concern about the alignment of education and what actually industry needs, an alignment that will require more long-term evaluation. In order to enhance the existing capacity cybersecurity education needs to be engrained through all stages of education and all staff in the public sector need to receive training in cybersecurity. Investment should be made into effective metrics that will ensure that educational offerings meet the needs of the cybersecurity environment.

Obviously there is a difference between education and skills. While there are cadres of experts that receive training in *cybersecurity skills*, this cadre is still too small to adequately meet the needs of British society. Our evidence suggests that the immediate need to increase capacity of UK companies in terms of cybersecurity is creating a short-term priority for skill development that the education sector is evidentially responding to. But this is emerging. Experts working in this field need to be more than IT professionals, enhancing skills such as the ability to understand security issues while building technology. As a result, at the moment there is a perceived skill shortage, emphasising the need for combining education and practical training. Therefore, there is a need for more investment in cybersecurity and skill development programmes.

Evidence suggests that there needs to be a broadening out of cybersecurity education from the technical and computer science disciplines across many more disciplines of education at all levels (in the appropriate ways). To progress, we would expect to see business management, philosophy, politics and international relations, public policy, defence and security, law, sociology, economics, ethics, to name but a few, to develop a consideration of cybersecurity within their syllabuses. Additionally, we would expect the public and private sector to establish basic requirements for cybersecurity training.

The review identified the *Legal and Regulatory Frameworks* as being at an *established* stage of maturity. ICT security legislation is particularly advanced and even reaches a *dynamic* stage, since comprehensive ICT security legislative and regulatory frameworks addressing

cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in the UK. A comprehensive structure within the criminal justice system is in place to combat computer-related offences while respecting human rights and the country is engaged and works with international organisations on privacy and data protection. The UK has ratified international treaties, such as the Human Rights Act, and other agreements to adopt appropriate legislation, in order to combat criminal offences against privacy and data protection, by facilitating their detection, investigation and prosecution.

Regarding *investigative capacity*, there are differences in the level of capacity and skills between local and national units due to a perceived lack of resources. During our consultation, it was raised as a concern that there is no existing procedural legislation for conducting cybercrime investigations and particularly cross-border investigations. In the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully prosecute cybercrime. A point raised by stakeholders was that there is no existing legislation for conducting an investigation. Whether this sort of legislation is required is still debated as some participants contended that existing legislation is sufficient, while others indicated new legislation is necessary to address challenges in cross border investigation. In order for the existing capacity to be enhanced we recommend the allocation of additional resources to cybersecurity education and training for prosecutors, judges and law enforcement as well as enhancing investigative capacity and skills locally.

There are schemes on cooperation and sharing information and *responsible reporting* with the private sector and SMEs, but there are no national regulatory standards for sharing incident information that companies are required to follow. However, it should be noted that the observations made in the *culture and society dimension* suggest that multi-stakeholder cooperation could be improved. Of particular question in the media, and hence in public discourse, is the issue of oversight in the UK. During the review we did not collect evidence that would suggest this is a solved problem; indeed, we would suggest that this is an on-going issue and one which will need to be addressed in order to progress maturity in other areas of capacity.

A vulnerability-disclosure framework is in place, and there is some ability to share technical details of vulnerabilities with other stakeholders who can distribute the information more broadly. Sharing of information can enhance situational awareness at an organisational but also at a national level. However, in the UK there is no compulsory reporting and information disclosure remains voluntary. This will have a significant adverse effect on the ability of the country to maintain a reliable national cybersecurity posture which can take account of day-to-day changes in threat and risk, beyond relying on key individuals and their personal contacts and knowledge of organisations, as noted above. In order to promote responsible disclosure we recommend the development of a responsible disclosure policy within the public sector and facilitate its adoption in the private sector through targeted outreach, by encouraging a cyber secure behaviour rather than its forcing adherence.

Finally, our consultations found the dimension concerning *Cybersecurity Standards, Business models and Technologies* in the UK to range from *formative to dynamic stages*. The evidence collected suggests that awareness and implementation of international *standards and best*

practices is at an *established* stage of maturity, but this maturity depends on the size of the enterprise. There are recommended standards to be adhered to but these are not consistently adopted. In order for the existing capacity to be enhanced a programme needs to be established to strengthen government's capacity to adapt or adopt international standards to all scales of industry; promote awareness and implementation of standards among SMEs; incorporate cybersecurity considerations in all stages of software and system development and processes; establish a process to measure the impact of standard adoption and conduct risk assessment exercises in order to inform adherence to select standards and embed security-by-design, in testing software.

Regarding *national infrastructure resilience*, technology and processes deployed meet international IT standards, guidelines and best practices. But, these processes have not reached a rigorous level for security risk management, threat assessment, incident response and business continuity. Moreover, there seems to be no business model implemented in a large scale to measure impact. Therefore, there is a need for enhancing the level of security processes in place (threat assessments and risk management processes); conducting regular assessments of processes and national information infrastructure security according to standards and guidelines and development of metrics to assess benefits for businesses from additional investments in technology

Concerning the *cybersecurity marketplace*, there are two main issues that we are looking at, a) cybersecurity technologies and b) cyber-insurance marketplace. After reviewing both aspects of this factor we have identified quite a large disparity between them. We need to acknowledge that cybersecurity technologies may reach a dynamic stage of maturity, while the cyber-insurance market is at a formative stage. There are cybersecurity products developed domestically and exported to other nations, indicating a high maturity in this area.

Also, the need for a market in cyber-related insurance has been identified through the assessment of financial risks for public and private sector. Insurance companies cover small issues but various types of harm are not typically covered, such as reputational harm. In general the insurance market is perceived as being limited by the lack of data upon which to develop models to underpin products. This is an international issue and not specific to the UK. Our evidence suggests that the insurance providers (in the broadest sense) are working on addressing these needs. However, in our view progress could be enhanced by the provision of good data, which itself could be underpinned by a change in the regulatory environment. Of course, we note that in many cases insurance products will not be sufficient risk mitigation for an organisation and we would expect companies to cease trading under particular brands due to the harm resulting from cyberattacks in the future. We would recommend that the UK undertakes a strategic consideration of the requirements for technologies and risk mitigation controls in the context of harm to the country – as it may be that a system's lack of view on how controls are being orchestrated across the country and/or within an enterprise could result in significant risk aggregation taking place, with the potential for future harm to national security and prosperity. We note that this is a general limitation in the area of cybersecurity capacity and not a deficiency unique to the UK – we would expect all countries considered to be leading the international community in terms of cybersecurity expertise to possess a need to address this capacity. The limited capacity in this market can be enhanced through promotion of information-sharing and good practice among organisations, to

enhance cover offered by cybercrime insurance while selecting cover based on strategic planning needs and identified risk.

Overall, it should be noted that the level of participation in the review by stakeholders was lower than we might have hoped for. Moreover, it was not possible to consult all stakeholder groups (such as the Intelligence Community and the Defence Community). This necessarily limits the comprehensiveness of the results and necessitates more reliance, in some areas, on desk research.

This was the ninth country review that we have supported directly, and the first of an *advanced* nation. As such, it visited a number of previously unexplored corners of the model and provided useful input into the evolution of the model. We note that participants generally (and commendably) refrained from stretching to claim higher levels of maturity than could be evidenced, and so we are confident that the assessments ultimately made are sound and possibly conservative.

We understand that the UK is in the process of developing different aspects of cybersecurity capacity including (but not limited to) revision of the National Cybersecurity Strategy, and that the UK aims for continuous engagement in international cooperation. These efforts will set the foundations for an advanced capacity in the future. We hope that this review, will offer useful insight to the UK and that our recommendations on how to increase cybersecurity capacity will contribute to the on-going work on the development of the UK National Cybersecurity Strategy 2016–2020.

Professor Sadie Creese
Director, Global Cyber Security Capacity Centre

Review of Cybersecurity Maturity

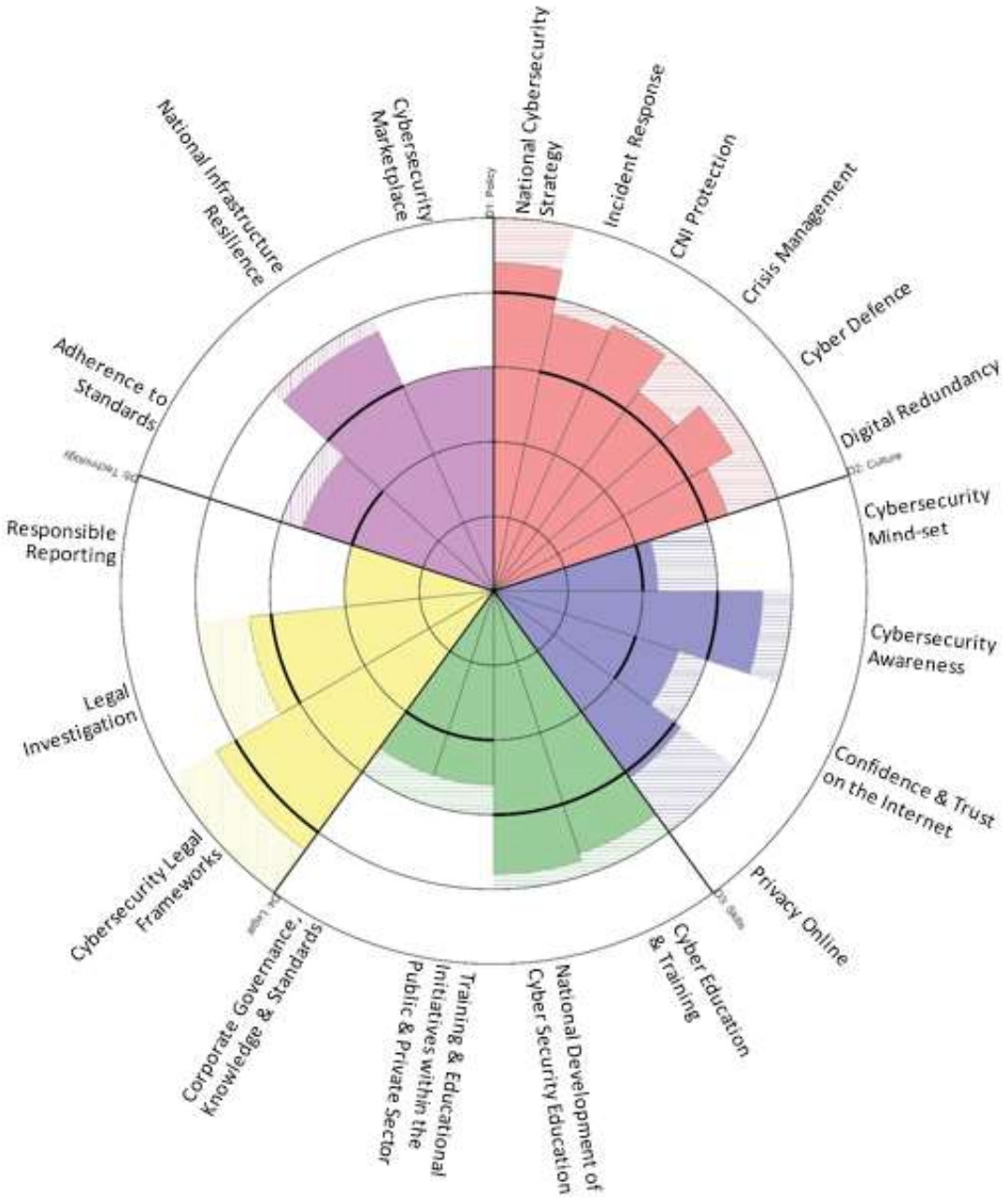
In this section we provide an overall presentation of the cybersecurity capacity in the United Kingdom. The graphic facing (Graphic I), presents the maturity estimates in each dimension. The stages of maturity for each factor extend out from the middle as an individual bar, and each dimension is a fifth of the graphic.

As seen in this graphic, based on the evidence collected, for the majority of factors cybersecurity capacity in the UK lies between an *established* and *strategic* stage of maturity. However, for certain factors, in Dimension 1 (Strategy and Policy) and in Dimension 4 (Legal and Regulatory Frameworks), maturity seems to be at a higher (dynamic) stage. Furthermore, as illustrated in the graphic, for a number of factors some evidence was gathered indicating activity at a higher stage of maturity. However, according to the methodology followed during the deployment of the Cybersecurity Maturity Model (CMM), the indicators for a certain stage need to be fully achieved for that stage of maturity to be assigned. Otherwise, maturity is recognised only at the highest completed stage. The assignment of maturity stages is based upon our interpretation of the evidence including the general or average view of accounts presented by stakeholders, desktop research conducted, and our professional judgement.

Black highlighted borders in the graph indicate the end of a stage. It is a simple matter therefore, to indicate where progress is already underway towards reaching the next stage of maturity in many indicators. Diagonal lines indicate the remaining areas of capacity required to reach the next stage of maturity for a particular factor.

Table I (see Appendix) presents a summary of the results on the stage of maturity for each factor, including a brief description of those results. Links to key policy and strategy documents, laws and other additional information are also provided in the Table. Table II (Appendix II) presents a total of eighty-four recommendations regarding the enhancement of the existing capacity for each factor.

Graphic I: Review Results



Dimension 1: Cybersecurity Policy and Strategy

Not every government has established a national level cybersecurity policy and strategy, or a body responsible for policy and strategic implementation. Cybersecurity as a policy area is still evolving. However, the importance of designating an overarching government body for cybersecurity coordination, and having a national cybersecurity strategy and policy cannot be overemphasized. It is widely accepted that those governments that have taken these measures are much better placed to cope with, and mitigate, cyber-incidents and attacks. This dimension explores the capacity of the government to design, produce, coordinate and implement a cybersecurity strategy.

D1-1: Documented or Official National Cybersecurity Strategy

Cybersecurity policy and strategy are essential to mainstreaming a cybersecurity agenda across government because they help prioritize cybersecurity against other important policy areas, determine areas of responsibility and mandates of key cybersecurity government actors, and direct allocation of resources to the emerging and existing cybersecurity issues and priority areas.

Stage: Strategic

The UK Government developed a National Security Strategy (NSS) in 2010, rating cyber-attacks as a 'Tier 1' threat. That strategy aimed to tackle threats in a way, which balances security and respect for privacy and fundamental rights. At home and internationally the UK government sought to ensure that cyberspace would remain an open space – open to innovation and free flow of ideas, information and expression. This strategy focused on reducing the risk and securing the benefits of a trusted digital environment for businesses and individuals. The vision of the UK Cyber Security Strategy 2011–2015 was to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where actions, guided by core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society. The objectives of the Strategy were for the UK: 1) to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace; 2) to be more resilient to cyber-attacks and better able to protect interests in cyberspace; 3) to help shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies; and 4) to have the cross-cutting knowledge, skills and capability needed to underpin all our cybersecurity objectives.

Multiple stakeholders implement the National Security Strategy across government. There is a review of and renewal process for the strategy, but not on an annual basis. Moreover, wider society and the private sector are not yet formally part of the process. There is a yearly review of the National Cyber Security Programme (NCSP), but in discussion with the authors of this report, stakeholders identified the need for a broader conversation with all stakeholders including the private sector, wider society and international partners. The review of the NCSP results in the allocation of budget according to perceived needs.

The National Security Strategy is only starting to take into account all levels that have to be considered, while translating the strategy to all governance levels (police forces, etc.). For

these reasons, all stakeholders agreed that the development of the National and Cyber Security Strategies is not yet at a dynamic stage.

Cybersecurity strategic plans drive capacity building and investments in security. The UK plans are strategic enough to secure and allocate investment. Appropriate metrics and qualitative assessment processes have been established, implemented and inform decision-making. The results of evaluating the existing metrics and assessments will influence the outcome and the review of the CSS. The programme at the Cabinet Office has the capacity to assess needs and threats and allocate funding accordingly. The ten high-level strategic objectives (derived from four overarching strategic goals in the CSS[2] described above) are adapted based on the effectiveness of these objectives, each with specific internal metrics.

There is evidence of iterative application of metrics and resulting refinements to operations and strategy across government departments and agencies involved in cybersecurity, including in the areas of risk assessment and management. However, differing mandates create a confusion of priorities and it is not clear how to separate responsibilities. As a result, there are different metrics for different aspects of the CSS. The main metrics used in the UK are a) the annual report on incidents[3] from CERT-UK and b) the NCSP team report on project management. These metrics do not assess risk, but rather assess how mature the reaction is. As a result, they assess reactive rather than proactive aspects of the strategy. They are more qualitative than quantitative and they focus on project management, rather than on cybersecurity properties or posture enhancements. During our consultation, it was noted by stakeholders that detecting incidents is not enough and that effective metrics are essential in order to provide a better understanding of capacity and cybersecurity posture as a nation.

The content of the CSS is revised in the light of metrics and measurements and evolving threats and lessons learned shape the implementation of the strategy. The budget can be quickly repurposed, as threats emerge, reprioritising resource investment. The government is now in the process of revising the CSS for 2015–2020, based on threats, lessons learned and the outcomes of the strategy implementation. While the stakeholders agreed that the UK is moving towards leading and promoting an internationally secure, resilient and trusted cyberspace, they also believed that it has a considerable way to go to accomplish this goal.

D1–2: Incident Response

This factor speaks about the capacity of the government to identify and determine characteristics of national level incidents, events or threats in a systematic way – preferably, through a central registry. It also reviews the government's capacity to organize and coordinate an incident response.

Stage: Established

It was observed by all stakeholders that there are incidents listed at a national level. A central registry of national-level cyber-incidents is established and held by CERT-UK. But there is no

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386094/Infographic_The_UK_Cyber_Security_Strategy_December_2014.pdf
[3] https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf

central regulation for incident response, and no mandate or protocol requiring incidents to be reported. There is an effort to be proactive in incident response, and the Cybersecurity Information Sharing Partnership (CiSP)[4], part of CERT-UK[5], regularly updates incident lists**.** While these efforts provide a structure for incident disclosure and collection, organisations also voluntarily report incidents to CERT-UK.

Furthermore, there is an official system for responding to threats and ensuring resilience. In the case of a cybersecurity related incident the Cabinet Office coordinates the response but it is the affected government department that leads the response. Although most government departments are prepared to report incidents and plan a response, there is no mechanism for capturing incidents at lower governmental levels, or locally. Although some entities have high capacity at a national level, they are not as mature. It was suggested by stakeholders that the local government sector has to step up and adopt new approaches regarding incident response.

It was agreed by stakeholders that the level of maturity of the UK's capacity for incident response depends highly on the organisations, the way they react to a threat and whether they will contact CERT-UK in case of an incident. Thousands of companies have already signed up to CiSP, sharing information on threats they face. Most of the larger companies are also aware that they can report incidents to CERT-UK and CiSP. CERT-UK also performs incident response exercises, but the capacity for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities and a zero-level incident alert will not be met for some years.

As far as coordination is concerned, the responsibility for incident response is allocated within each public administration entity, governmental department and ministry. At this point, there is cooperation between public and private sector. As stated above, CERT-UK and CiSP provide a structure for incident disclosure and collection for private sector. For incident response a number of smaller departments would contact the Cabinet Office[6] [7]. During an emergency, one of two senior decision-making bodies within COBR[8]—the Strategy Group or Civil Contingencies Committee[9]—will usually be activated. In an emergency where a central

[4] https://www.cert.gov.uk/cisp/
[5] https://www.cert.gov.uk/
[6] Cabinet Office, *Responding to Emergencies: The UK Central Government Response: Concept of Operations,* 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192425/CONOPs_incl_revised_chapter24_Apr-13.pdf
[7] Cabinet Office, Civil Contingencies Secretariat. *The Lead Government Department and its role – Guidance and Best Practice.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61355/lead-government-departments-role.pdf
[8] COBR (Cabinet Office Briefing Room) is a forum of Ministers and senior officials from relevant Departments and agencies, brought together to make decisions on an emergency response. External representatives and experts are invited to attend COBR meetings as appropriate; discussions are classified.
[9] Emergency Response and Recovery Non statutory guidance accompanying the Civil Contingencies Act 2004 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/253488/Emergency_Response_and_Recovery_5th_edition_October_2013.pdf

response is required, a Lead Government Department (LGD)[10] is appointed. CERT-UK will also provide advice to entities or alternatively direct them to CREST[11].

D1-3: Critical National Infrastructure (CNI) Protection

This factor studies the government's capacity to identify CNI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CNI asset owners, and enable comprehensive general risk management practice including CNI risk management.

Stage: Established

At a national level, there is a list of identified Critical National Infrastructure assets, but respondents expressed concerns as to its accuracy. The Treasury also keeps a list of CNI assets, which is reviewed on an annual basis.

At the national level CNI assets are clearly determined and categorised and risk management exercises are conducted. But this is not the case at lower levels where there is not a specific analysis of assets. Respondents stated that for local government, there are differences in priorities and on the processes followed.

Defined reporting requirements between CNI asset owners and the public sector, as specified by the Centre for the Protection of Critical Infrastructure (CPNI)[12], are sufficient to address national security needs. Regulators cooperate with ministries and agencies, but the majority of stakeholders stated that very few regulators have specific cyber-incident response regulations and different regulators will translate the need for resilience differently. For example, the banking sector has a long history of using digital data and has evolved to an understanding of different security needs, whereas for, the energy sector, there are no cyber-reporting requirements.

HM Treasury, other government agencies, and financial authorities have formed a Cross Market Operational Resilience Group (CMORG), which works on assessing, testing and improving cyber-resilience across the core parts of the UK financial sector and on building a structure to connect different stakeholders at different levels. The telecommunications sector has developed a similar structure, namely, the high-level governmental security group called the Telecommunications Industry Security Advisory Council (TISAC)[13].

TISAC was established by the Cabinet Office Central Sponsor for Information Assurance (CSIA), which became part of the Office of Cyber Security (OCS) in 2009, to discuss and respond to threats to UK telecoms resilience. TISAC includes senior executives and chairmen of communications providers, operators, internet exchanges, telecoms regulator Ofcom, the OCS, and the Department for Business, Innovation and Skills (BIS).

[10] The Cabinet Office maintains a list of LGDs that sets out where the lead should lie in both the response and recovery phases for a wide range of emergencies.
[11] http://www.crest-approved.org/
[12] http://www.cpni.gov.uk/
[13] http://itlaw.wikia.com/wiki/Telecommunications_Industry_Security_Advisory_Council

The severity of the effect of incidents on critical assets is informed by regular exercises and assessments. Routine mechanisms for review of the response process are also in place. The majority of stakeholders agreed that response planning varies depending on the sector involved. Different environments follow tailored paths and strategies regarding incident response. The finance sector has longer experience and knowledge in this.

It was evidenced that CERT-UK and GOV CERT have more capacity in response planning. During our data collection stakeholders noted that at a national level, the UK has not faced a cybersecurity related incident with large scale effects. However, we have to acknowledge that there is a trend of attacks in various sectors and these incidents are being disclosed. The level of support regarding incident response from the government depends on the expected impact that the incident will have.

As far as coordination is concerned, there are mechanisms for communication between different sectors, but this also depends on the organisation and varies across sectors. Central bodies and mechanisms have been established, but audit functions to address risk, are not fully developed yet. There is a Cyber Communications Group and legal departments feed into that group. Moreover, it was stated that the implementation of communication strategies is ad-hoc.

Risk management is considered and security measures and guidelines for CNI cybersecurity best practice have been established, but usually only telecommunication and energy companies have advanced capabilities to detect, identify, protect, respond and recover from cyber-threats. Insider threat detection is also an issue of high importance for CERT-UK.

The CiSP platform, supported by CERT-UK, helps sharing information, although there is no legal obligation to do so. It was agreed among stakeholders that more legislation relating to disclosure for organisations would actually prevent cooperation since a legal requirement to disclose information might lead companies to cease attempting to detect incidents. Stakeholders felt that a voluntary information disclosure policy would encourage better information sharing. However, some believe that voluntary disclosure will not work. To avoid behaviours, which avoid detection of events, any legislation would need to encompass both a detection requirement and a disclosure requirement. We note that creating such a package will require thought across standards, skills and technology.

D1-4: Crisis Management

Crisis management planning and evaluation capacity, bolstered by functional protocols and standards, is critical to implementing cybersecurity policies that are results-oriented and sustainable. Crisis management planning usually entails, but is not limited to, conduct of specialized needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.

Stage: Established

In the UK the importance of planning and evaluating crisis management applications is well understood. CERT-UK conducts national level exercises and more sophisticated exercises are already planned for forthcoming years. There is capacity within these exercises to simulate real world scenarios, but it was noted that there are not enough live technical exercises at a national level. Stakeholders agreed that recognition of the importance of crisis management exercises is lacking, especially at a local level, while the biggest challenge is to communicate the value of these exercises. Another issue raised was that real-world impact would not necessarily be cyber-limited or related - an observation which needs to feed into cyber-crisis management exercises.

The ownership of the lessons collected from exercise evaluations is also important. Issues such as real impact of an attack and resilience against an attack are part of the exercise evaluations. There are reports at a national level regarding lessons learned but these are policy oriented rather than operational. These reports will then influence the strategy of CERT-UK. Stakeholders mentioned the difficulty in engaging people to participate in the evaluation process, unless an incident has occurred.

D1-5: Cyber Defence Consideration

This factor explores whether the government has the capacity to design and implement a cyber-defence strategy and lead its implementation including through a designated cyber-defence organisation within the executive branch. Among other considerations, it also reviews the level of coordination between various public and private sector actors in response to malicious attacks on military information systems and critical national infrastructure.

Stage: Established

There is no dedicated Cyber Defence Strategy in the UK but through the Cyber Programme[14], key documents including, the National Strategic Defence and Security Review[15] and the National Security Strategy[16] are all used for this purpose. Furthermore, in March 2008 the UK Government published "*The National Security Strategy of the United Kingdom: Security in an interdependent world*"[17], while in 2010, the government published a new National Security Strategy "*Strong Britain in an Age of Uncertainty: a Strategic Defence and Security Review (SDSR)*"[18]. These documents refer to the National Security Strategy.

The UK's 2011 Cyber Security Strategy characterises cyber-attacks as "*a national security threat, and aims, inter alia, at defending national infrastructure from cyber-attacks and improving capabilities to deter and disrupt attacks on the UK*". Within the Ministry of Defence, a Global Operations and Security Control Centre and a Defence Cyber Operations Group

[14] https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf
[15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf
[16] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf
[17] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf
[18] https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

defend the Ministry's network, integrating the MoD's cyber-activities across the spectrum of defence operations. In 2013, the UK announced its intention to incorporate cyber warfare as part of future military operations and to develop a "cyber strike force" to respond to potential military use of cyber capabilities. The current MoD research focuses on automated cyber-defence response systems. Research driven in the area is being partly run by the Defence Human Capability Science and Technology Centre (DHCSTC), which is administered by BAE, in parallel with various DSTL related research initiatives and also CDE Programmes aimed at fostering innovation in this space.

The 2015 National Security Strategy and Strategic Defence and Security Review (SDSR) were published in November 2015 (after the completion of the evidence-gathering phase of this review), drawing upon work by the GCHQ Centre for Cyber Assessment.

Military defences have highly specialised expertise with advanced strategic cyber-capabilities. National Cyber Defence coordination in response to malicious attacks on military information systems and critical national infrastructure is mainly performed by the Ministry of Defence's CERT (MoD CERT) and by the CERT-UK for attacks on CNI. Also, the MoD Joint Forces Command[19] works towards making military operations successful by making sure that joint capabilities, such as medical services, training and education, intelligence, and cyber-operations, are efficiently managed and supported. They also communicate actual experience in operational theatres so that it can be reflected in top-level decision-making.

The University Short Course Programme (USCP)[20] forms part of the wider strategy of the Services to contribute to the improvement of the general education of Service personnel. USCP intends to help Service personnel develop their knowledge and personal skills. This is achieved through personnel having the opportunity to address matters of current importance and research and development, such as cybersecurity, within an academic environment.

Another important part of the Army Forces is the Army Reserve[21]. The Army Reserve provides highly trained soldiers who can work alongside the Regulars on missions in the UK and overseas. Secondly, it gives people who have specialist skills, including skills related to cybersecurity, a range of opportunities to use them in new ways. In 2013, the MoD announced the creation of a new Joint Cyber Reserve[22], which will see reservists working alongside regular forces to protect critical computer networks and safeguard vital data. The Cyber Reserves will be an essential part of ensuring defence of national security in cyberspace and protection of vital computer systems and capabilities. The creation of the Joint Cyber Reserve will represent a significant increase in the number of reservists employed in cyber and information assurance, and members of the Joint Cyber Reserve will provide support to the Joint Cyber Unit (Corsham), the Joint Cyber Unit (Cheltenham) and other information assurance units across Defence. The Joint Cyber Reserve will be in place by April 2017.

[19] https://www.gov.uk/government/organisations/joint-forces-command/about
[20] http://www.army.mod.uk/documents/general/20150625-ShortCourseProspectus-PRINT-O.pdf#search=cyber war
[21] http://www.army.mod.uk/reserve/31781.aspx
[22] https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

D1-6: Digital Redundancy

Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network). This factor reviews a government's capacity to plan and organize redundancy and redundant communications among stakeholders.

Stage: Established

In the UK, emergency response asset priorities and standard operating procedures are established in the event of a communication disruption in the emergency-response network, including ensuring that back-up centres are in place. The Department for Culture, Media and Sport is responsible for the resilience of the communication sector. Communication is distributed across different parts of the response network, such as the emergency response functions, the public and private responders, and command authorities.

It was agreed among stakeholders that the private sector is more advanced regarding digital redundancy. This is why there is an effort to enhance cooperation between public and private sector in cyber-specific work.

Recommendations

Following the information presented during the review of the maturity of *Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations to be considered by the government. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

As stated, the UK National Cybersecurity Strategy review and renewal processes are confirmed. The government is now in the process of revising the national cybersecurity strategy (2015–2020), based on threats, lessons learned and outcomes of the strategy implementation. However, during the revision all levels of authority need to be taken into account. Another important issue is that differing mandates create a confusion of priorities and it is not clear how to separate responsibilities. As a result, there are different metrics for different aspects of the national security strategy. Additionally, detection of incidents is rather reactive and this is why effective metrics are essential and necessary in order to provide a better understanding of a more proactive capacity. Therefore, we provide the following recommendations:

- R1-1: Develop the capability to modify the content of the strategy in response to the cybersecurity environment regularly and incorporate it in the strategic plan.
- R1-2: Encourage a broader conversation with all stakeholders including the private sector, wider society and international partners during the yearly review of the National Cyber Security Programme (NCSP).
- R1-3: Set a mechanism in place to implement the strategy in full scope, including at a local level.

- R1-4: Enhance the capacity for adapting focus on incident identification and analysis in response to environmental changes.
- R1-5: Develop predictive methods to assess risk, its propagation and its aggregation for the National and CNI lens.

Regarding incident response there is no regulation and no mandate authority or protocol requiring incidents to be reported. Although most of the governmental departments are prepared to report incidents and plan a response, there is no mechanism for capturing incidents at lower governmental levels, locally. It was suggested by stakeholders that local government has to adopt new approaches regarding incident response. Hence we suggest the following:

- R1-6: Incorporate an early warning capacity into the mission of the emergency response organisation.
- R1-7: Embed tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities in emergency response organisation(s).
- R1-8: Prioritise multi-level national coordination between all levels and sectors to incident response at regional and international level.
- R1-9: Prioritise drafting regulations on incident response, and promoting reporting of incidents.
- R1-10: Appoint a mandate authority to ensure reporting of incidents.
- R1-11: Develop a mechanism of capturing incidents on lower governmental levels, locally.

At the national level CNI assets are clearly determined and categorised and risk management exercises are being conducted. But this is not the case at lower levels where there is not a specific analysis of assets. At the local level, there are differences in priorities and on the processes followed. Regarding incident response different environments follow tailored paths and strategies. As far as coordination is concerned, there are mechanisms for communicating between different sectors, but these also depend on the type of organisation and vary across sectors. We suggest the following:

- R1-12: Develop a mechanism of asset analysis on lower governmental levels, locally.
- R1-13: Prioritise listing of CNI assets and regularly re-appraise to capture changes in the threat environment.
- R1-14: Invest in capability of Board Members and Senior Leaders of organisations to understand cyber-risk intelligence, so that they can lead in the face of crisis and take their part in risk management more generally.
- R1-15: Implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio.
- R1-16: Strengthen formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector.
- R1-17: Execute procedures to optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations as needed to encompass incident prevention, detection and response.

Regarding crisis management planning and evaluation there is a lack of recognition of the importance of crisis management exercises, especially at a local level, while the biggest challenge is communicating the value of these exercises. There are reports on the lessons collected from exercise evaluations at a national level but these are policy oriented rather than operational. Therefore, we recommend the following:

- R1-18: Prioritise crisis management exercises, especially at a local level, and communicate the value of the exercises.
- R1-19: Conduct compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises to inform strategic investment in future emergency response assets.

As noted, there is no dedicated Cyber Defence Strategy in the UK, but through the Cyber Programme, the National Strategic Defence and Security Review and the National Security Strategy are being utilised for this purpose. Some recommendations in order to enhance cyber-defence capacity are:

- R1-20: Draft a Cyber Defence Strategy.
- R1-21: Enhance funding efforts for research and development focused on automated cyber-defence response systems, and speed up time to operational impact. Consider developing a performance assessment environment for assessing performance of methods in a non-classified environment, to support procurement and on-going requirements development.
- R1-22: Conduct constant review of the evolving threat landscape in cybersecurity to ensure that cyber-defence policies continue to meet national security objectives.
- R1-23: Prioritise compliance of the National Security Strategy and National Strategic Defence and Security Review with international law and consistency with national and international rules of engagement in cyberspace.

Digital redundancy planning is highly advanced, especially within the private sector. There are efforts to promote cooperation between public and private sector regarding digital redundancy. Regarding the enhancement of the existing capacity it is recommended to:

- R1-24: Enhance cooperation between public and private sector in cyber-specific work and specifically digital and non-digital systems redundancy.
- R1-25: Communications and emergency response assets need to have both non-digital network backups and access to personnel trained to activate and maintain them.

Dimension 2: Cyber Culture and Society

Even the most forward-thinking cybersecurity strategies and policies are of little help if actors not formally charged with enhancing cybersecurity do not understand their roles and responsibilities. Users and other stakeholders play critical roles in safeguarding sensitive data and protecting their personal and organisational resources as they interact through digital means. This dimension reviews important elements of a responsible cyber-culture and society at the individual and organisational level as perceived by a variety of stakeholders. Important cultural and social aspects supportive of cybersecurity include the level of trust in Internet services, such as in e-government and e-commerce, and adherence to privacy aware practices in handling personal information by all the entities that engage in provision of these services. All cybersecurity experts need to avoid blaming users for problems with cybersecurity. Instead, experts need to build useable systems and programs and also ensure that users are aware of threats and good practice, and know how to incorporate good practices into their routine behaviour online.

D2-1: Cybersecurity Mind-set

This factor evaluates the degree cybersecurity is prioritized and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mind-set is understood as a predisposition and, in certain cases, as a consistent, routinized behavioural pattern in aligning one's actions with good cybersecurity priorities both at an individual level and in an organisational setting. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Formative

Cybersecurity has been recognised as a priority across the UK government, and therefore risks and threats are taking a role in building a cybersecurity mind-set in the country. At a governmental level, cybersecurity is a widespread concern, but there are variations across departments and levels of the government, such as between departments that have traditionally handled personal information, and those that have not. After consultation with stakeholders from government, it was suggested that there are some agencies that are aware of cyber-risks, while others are less aware. Agencies that focus mostly on cybersecurity, such as CERT-UK and the Government Communications Headquarters (GCHQ), actively promote a cybersecurity mind-set, but more work needs to be done. For example, government departments in the UK have been briefed on the "*10 Steps to Cyber Security*"[23] and have been informed of the threats. The language of cybersecurity is evident in all departments. Nevertheless, issues emerging from interviews included:

- A more reactive rather than proactive approach to cybersecurity in government, such as a cybersecurity mind-set and consciousness of the secure use of online systems arising as the outcome of an attack.

[23] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

- An insufficient understanding of cybersecurity risks, particularly at lower levels of the government.

As a result, the cybersecurity mind-set in government remains at a formative stage, but there is an on-going self-assessment process taking place, which holds promise for informing and changing practices.

Within the private sector, high-risk practices are being identified. However, there are differences across the various industries and the scale of an organisation also contributes to this difference in understanding. Larger organisations are more often aware of cybersecurity risks and therefore more likely to prioritise cybersecurity in their risk management approach. SMEs, on the other hand, do not have the same cybersecurity mind-set because their perception of cyber-threats is not given as high a priority. There are sectors where employees have a proactive mind-set, but in general, smaller companies feel most vulnerable, yet lack a strong sense of secure practices. Generally, businesses are concerned about cybersecurity, but very often they are unsure of the actions they can and need to take. Companies often react when there is a business problem or an attack, rather than engaging proactively in building their cybersecurity capacities. Incidents, then, are the major reason for employing cybersecurity practices. Stakeholders during the consultation agreed that companies sharing information on incidents and learning from others' experiences might support a proactive cybersecurity mind-set.

Individuals across society-at-large, according to stakeholders, inconsistently adopt a cybersecurity mind-set. Programmes and materials have been made available to train and improve cybersecurity practices and there is a growing effort towards raising awareness in schools and workplaces. Nevertheless, the majority of individuals in the UK are not fully aware of the possible risks online and even increased awareness over time does not necessarily mean society is more cyber secure, if users do not have clear approaches to protecting their security. It was agreed that although awareness might exist, the appropriate actions are not necessarily understood or taken.

Another issue raised was the gap between concepts of cybersecurity between experts and other members of society, and how that difference might influence practices. Experts often have unrealistic expectations of the ordinary user. Instead of blaming users for not following cybersecurity practices, such as resetting passwords, there is a need for developing practices that are easier for users to adhere to, and putting more resources into ensuring a broad understanding of threats and means for addressing them. There is a growing awareness movement across civil society in the UK, but realising a shift to a more cyber secure mind-set remains a long-term goal.

D2–2: Cybersecurity Awareness

This factor focuses on the prevalence and design of programs to raise cybersecurity awareness of cyber-risks and threats as well as how to address them. Awareness raising programmes need to cover a wide range of target groups of society, particularly children in different age groups and other vulnerable groups, and their effectiveness should be observed and measured.

Stage: Established

Publicly oriented awareness-raising initiatives are increasing in the UK, along with a sense of a growing awareness of the risks. For example, the national coordinated cybersecurity campaign "*Cyber Streetwise*"[24] is a joint departmental initiative that tries to drive behavioural change by providing tips and advice on how to improve online security. The campaign targets both Internet users in households and businesses. There is a high level of multi-stakeholder engagement in this effort, especially in the delivery of the awareness campaign, but less so in its design. The effectiveness of "*Cyber Streetwise*" is being measured through the reporting of cybercrime and these metrics are being used to inform the allocation of resources. At the same time, there are limits to the effectiveness of such measurements, given known problems with accurately measuring the prevalence of cybercrime, such as a reluctance of users, particularly businesses, to report cybercrime.

There are other significant awareness efforts, such as "*Cyber Essentials*".[25] This is also a coordinated, government-backed, industry-supported scheme to help organisations protect themselves against common cyber-attacks.

Moreover, CERT-UK, GOV CERT, the National Crime Agency (NCA) and other departments are coordinating efforts to build wider awareness across society. CERT-UK is responsible for training, with particular focus on CNI matters and the use of the CiSP, and circulates shared information and best practices for organisations. The programme "*10 Steps to Cyber Security*" is also part of the effort for raising awareness for SMEs.

Other coordinated programmes include the "*GetSafeOnline Campaign*"[26] which focuses on users at home and in business. This campaign is a jointly funded initiative between several governmental departments and private sector businesses. In addition, the "*Webwise Campaign*"[27] focuses mainly on parents and users in households to provide basic knowledge on various cyber-risks and tips on how to avoid these problems.

It was agreed by various stakeholders that it is important for the private sector to provide awareness education. However, companies often lack the resources to devote to building awareness on cybersecurity. Usually, the financial sector organises campaigns in order to increase their customer's basic level of awareness, but other sectors have yet to take such proactive measures. Businesses also face concerns over frightening their customers, if they create a disproportionate level of concern. Additionally, it was generally agreed that despite the on-going implementation of cybersecurity awareness-raising, campaigns do not

[24] www.cyberstreetwise.com
[25] http://www.cyberstreetwise.com/cyberessentials/?&nginxId=263c74e8-f8c9-45e1-c5e2-c51e4e1dd520
[26] www.getsafeonline.org
[27] http://www.bbc.co.uk/webwise/0/

necessarily cover all target groups, given that many specific groups face particular problems, such as bullying among young Internet and mobile users.

Metrics for observing the effectiveness of campaigns are established for many of these efforts, but not to a degree where they inform future campaigns taking into account gaps or failures from previous efforts. Finally, efforts such as the *Gloucestershire Safer Cyber Forum (GSCF)*[28] have been designed to provide a source of crime prevention, advice and to share cyber-threat information. This effort seeks to measure cybercrime prevention efforts at a local level.

D2-3: Confidence and Trust on the Internet

This factor reviews the level of stakeholders' trust in the use of online services, in general, and e-government and e-commerce services, in particular. Users need to be aware of cybersecurity risks, but not become so fearful that they are reluctant to try and use valuable online services.

Stage: Formative

Trust is a complex issue. Distrust of online services can undermine their use. For example, those most distrustful of the Internet are those who have never used it[29]. At the other extreme, blind faith in the Internet could lead to unsafe practices. As online services are being used increasingly, especially by younger users, trust does not necessarily continue to grow as many have negative experiences online. It was noted by various stakeholders that people tend to trust online services regardless of cybersecurity considerations when they have not had negative experiences. People like the convenience and immediacy of online services, despite cybersecurity risks. At an EU level there are many efforts regarding promotion of trust in online services. Also at a national level there is an identified effort to enhance trust of online services in ways that retains a healthy awareness of potential risks.

Companies are making a significant effort to shift their services online, but there is no coordinated programme on trust building beyond efforts to get users online so that they can directly experience the service. Internet Service Providers (ISPs) do not advertise their products based on security, since this could be off-putting to their customers, but rather on the speed of connectivity and ease of use, which might at times conflict with security if not well designed. ISPs know that they have to provide a sense of security in order for users to make use of their services, but security has yet to become a factor distinguishing one ISP from another that would make it a selling point for their users.

During this review, stakeholders agreed that this factor is at a formative stage, but fulfils part of the established stage of capacity. Research on users indicates that trust in the Internet is less among more educated users, who are more sceptical generally, but that trust grows with experience in using the Internet, unless users have negative experiences online. In short, trust in the Internet may be increasing whether or not service providers seek to promote security.

[28] https://www.safercybergloucestershire.uk/

[29] Dutton, W. H., and Shepherd, A., (2005) 'Confidence and Risk on the Internet', pp. 207-44 in R. Mansell and B. S. Collins (eds) *Trust and Crime in Information Societies*, Cheltenham: Edward Elgar Publishing.

In fact, many providers may worry that advertisements seeking to ensure that users feel secure online could have the opposite impact – raising doubts in their minds.

E-government services are being used widely in the UK and recognition of the need for the application of security measures to promote trust in e-services is recognised. However, there is no coordinated programme to promote trust in e-government services. In this area, the primary emphasis is on encouraging citizens and residents to use e-government services.

Also, the recognition and promotion of trust in e-government services depends on the department or the amount or kind of information provided online. Moreover, during this review it was identified that there is a difference between local and national government on this issue. There is a perception that local-government e-services tend to be more trusted by users than national e-government services and that is due to the ability of local government to promote the services they provide online, and potentially for users to communicate easily with departments if they face challenges with the services.

Stakeholders generally perceive UK e-government services to be at a relatively high-level of maturity but not yet fully mature. This remaining gap is often identified with a need for more attention to be placed on the protection of personal data and the anonymity of users.

E-commerce services are more fully established in a secure environment, while multiple stakeholders continue to invest in e-commerce. While companies see the need for secure systems to protect their business and customer data, there is no feedback mechanism to provide evidence on trust in e-commerce services. Differences in trust in e-commerce services depend on each different sector. The financial sector works towards promoting trust as well as securing their systems. A concern raised during discussions was the fact that the younger population is not sensitised enough on privacy issues and continues to make use of e-commerce services. However, the use of online commerce has continued to grow, indicating a relatively high evaluation of the services provided by the major e-commerce firms. It is therefore important to distinguish between the practices of, and trust in, the large e-commerce providers, and the small businesses and enterprises trying to establish themselves in the e-commerce arena, which might be most negatively affected by concerns over their security.

D2-4: Privacy Online

This factor reviews the salience of issues concerning the protection of personal data as illustrated by the government agenda through enactment of relevant practices, laws, and regulations, and the level of engagement and advocacy around them by civil society. It also evaluates how national legislative norms adhere to regionally and internationally recognised standards for human rights.

Stage: Established

The government adheres to regionally and internationally recognised standards for human rights (as discussed below in Dimension 4), in relation to privacy. The UK is an international leader in promoting Human Rights and government level officials understand the importance of privacy online. The UN Universal Declaration of Human Rights, the European Convention

for the Protection of Fundamental Human Rights and Freedoms, the Budapest Convention Art. 32 and Data Protection Act are being adhered to. The Internet Governance Forum and the UK Internet Governance Forum, illustrate a level of debate on issues such as privacy online that is not characteristic of most other nations. Likewise, Britain participates actively in the Internet Engineering Taskforce (ITF) that addresses privacy as an important issue and works on applying privacy standards in all online services. Civil society in the UK is actively driving change on this issue.

There are coordinated efforts regarding regulation in privacy standards within law enforcement. The UK's independent data protection authority, the Information Commissioner's Office (ICO)[30], was set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Also, the Interception of Communications Commissioner's Office (IOCCO)[31] is responsible for keeping under review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. IOCCO reports to the Prime Minister on a half-yearly basis with regard to the carrying out of the Interception of Communications Commissioner's functions.

However, while the UK government appears to be conscious about human rights, such as in drafting new laws and regulations, there is debate across civil society over whether security has been prioritised in ways that might compromise strong privacy and data protection. Finding ways to ensure security without trading off the protection of other values, such as privacy, is an increasing focus of most advanced liberal democracies faced with growing concern over such issues as terrorism and cybercrime, but also over surveillance. Debate over these issues in the UK is open and has the potential to lead to constructive directions for policy and practice.

For example, during the consultation, an issue raised was that privacy is less well understood within local government, and that standards and policies do not necessarily translate into day-to-day practice. Clearly, in emerging security measures being discussed in the UK, many see threats to the privacy of personal information as a direct consequence of efforts to enhance security. Comparable issues are arising in commerce around the use of personal information by third parties, such as for marketing, which also raises concerns over privacy and surveillance. This developing privacy-security tension in government and business needs to be a focus of attention in developing responsible personal data and security practices in both sectors, along with efforts to avoid these risks being politicised.

Consultations also identified privacy in the workplace as an important component of cybersecurity. While access to information in the workplace is very different than, for example, government access to information about households, there have been issues raised over surveillance in the workplace. Many employers maintain privacy policies that provide a minimum level of privacy for employees. Moreover, employees are sensitised to their privacy rights within the organisation. The Data Protection Act drives this issue, but in general there are different employee policies across different sectors.

[30] https://ico.org.uk
[31] http://www.iocco-uk.info/default.asp

Many small companies recognise the importance of the Data Protection Act but implementation varies across companies. Governmental departments are more visible, accountable, and perceive themselves to be more compliant than industry counterparts in this regard. Across governmental departments, employee privacy is being promoted and employees generally trust that their personal data will remain protected. In the private sector, there is also accountability, where privacy breaches can threaten a company's future. However, most attention is focused on companies protecting data about their customers, rather than their employees, so this area may need more scrutiny.

Recommendations

Following the information presented during the review of the maturity of *cyber-culture and society*, the Global Cyber Security Capacity Centre has developed the following set of recommendations:

At a governmental level, cybersecurity is a concern but there are variations in cultures and practices across departments at different levels of the government, such as departments that have traditionally handled personal information, and those that have not. As a result, there are some departments for which approaches to cybersecurity are more reactive than proactive, such as would be fostered by a stronger cybersecurity mind-set. Too often, consciousness of the importance of secure use of online systems arises as the outcome of an attack. Moreover, there could be a stronger understanding of cybersecurity risks, threats, and remedies across all levels and departments of government.

Within the private sector, many of the major differences in understanding of risks depend on the scale of the organization. Larger organisations are more aware of cybersecurity risks and therefore prioritise cybersecurity in risk management. Within society at large it seems that although awareness might exist, the appropriate actions are not necessarily understood or taken. Regarding the promotion of a cybersecurity mind-set within all sectors we recommend the following:

- R2-1: Enhance efforts at all levels of government to promote understanding of risks and threats, but also the design of systems that enable users across society to easily embed secure practices into their everyday use of the Internet and online services.
- R2-2: Promote sharing of information on incidents and best practices among organisations to promote a proactive cybersecurity mind-set.
- R2-3: Promote prioritisation of risk and threat understanding for SMEs.

As noted above, there are coordinated awareness-raising programmes in the UK, aligned with the National Cybersecurity Strategy and there is evidence of significant multi-stakeholder engagement in these efforts. Additionally there are metrics to assess the effectiveness of these efforts. At the same time, the effectiveness of such measurements is often limited due to difficulties in reporting cybercrime, such as online theft. Also, despite the on-going implementation of cybersecurity awareness-raising, campaigns do not necessarily cover all target groups. Regarding the enhancement of the existing capacity we recommend the following:

- R2-4: Maintain and expand the existing awareness programmes to cover various target groups (such as children, parents, experts, SMEs, government agencies) linked to the national cybersecurity strategy.
- R2-5: Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures.
- R2-6: Promote awareness of risks and threats at lower levels of the government.
- R2-7: Promote a high level of multi-stakeholder engagement in the design of awareness campaigns.
- R2-8: Encourage the private sector to provide awareness education.

Trust in online services seems to be high regardless of cybersecurity considerations. Companies are making a significant effort to shift their services online, but there is no coordinated programme on trust building. Additionally, there is no coordinated programme to promote trust on e-government services. While companies recognise the need for secure systems to protect their business and customer data, there is no feedback mechanism to provide evidence on trust in e-commerce services. In order to enhance the level of trust in secure online services we suggest the following:

- R2-9: Promote trust in e-government and e-commerce services through regulation ensuring personal data privacy and adherence of e-government services to the highest cybersecurity protection standards.
- R2-10: Develop a feedback mechanism to provide evidence on trust in e-government and e-commerce services, while helping users to understand the complex relationships between trust and use of the Internet.

There is a high level of debate on issues such as privacy online in the UK. This is important at this time given unresolved concerns over whether or not inappropriate trade-offs are being made to protect security that might lead to unwarranted surveillance or loss of privacy. Also privacy appears to be less well understood across local government, where standards and policies do not necessarily translate into day-to-day practice. Additionally, there is a concern that the younger population is not sensitised enough on privacy issues, even though the evidence is still mixed on this issue. Privacy in the workplace is recognised, as an important component of cybersecurity and employers should develop privacy policies that provide more than a minimal level of privacy protection for employees. Therefore we recommend the following:

- R2-11: Promote understanding and implementation of privacy standards and policies within local government.
- R2-12: Sensitise employees on their privacy rights and obligations within the organisation.
- R2-13: Sensitise all sectors of the public to privacy and data protection issues, including youth but also other vulnerable groups.

Dimension 3: Cybersecurity Education, Training and Skills

This dimension reviews the availability and quality of cybersecurity education, training, and skills in the UK for various groups of government stakeholders, private sector, and the population as a whole. In particular, it evaluates existing educational offerings and national development of cybersecurity education; training and educational initiatives within public and private sector; and corporate governance, knowledge, and standards.

D3-1: National Availability of Cybersecurity Education and Training

This factor speaks to the importance of availability of high quality cybersecurity education and training options, their integration and synergies, in order to ensure adequate and sustainable supply of cybersecurity skills for the needs of public and private sectors. It takes stock of existing educational offerings in schools and universities and training offerings within private sector and beyond it in the field of information security and cybersecurity and provides a superficial evaluation of their structure and components.

Stage: Established

There are educational offerings in cybersecurity at the national and institutional levels, ranging from primary to post-graduate, including vocational education in modular form. At a postgraduate level there are more offerings in cybersecurity than at an undergraduate level. Many universities offer different types of cybersecurity courses but not many of them have actual affiliation to industry.

The launch of GCHQ online training[32] available to all has shown intention to drive interest in education in cybersecurity. The National Cyber Security Strategy recognises education as key to the development of cybersecurity skills and UK universities were invited to submit their cybersecurity Master degrees for certification against GCHQ's rigorous criteria for a broad foundation in Cybersecurity.

Partnerships have been key throughout the process with the assessment of applicants based on the expert views of industry, academia, professional bodies, GCHQ and other government departments. The six successful Master degrees were judged to provide well-defined and appropriate content, delivered to the highest standard. The development of GCHQ-certified Master degrees will help universities promote the quality of their courses and assist prospective students to make more informed decisions when looking for a highly valued qualification. It will also assist employers to differentiate between candidates when employing cybersecurity staff.

GCHQ and the *Engineering and Physical Sciences Research Council* (EPSRC) have set up a scheme to recognise *Academic Centres of Excellence*[33] [34] *in Cyber Security Research* (ACEs-

[32] http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-certifies-Masters-Degrees-in-Cyber-Security.aspx

[33] http://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx

[34] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/296010/bis-14-660-developing-our-capability-in-cyber-security-academic-centres-of-excellence-in-cyber-security-research.pdf

CSR). To date 13 UK universities have been accredited as conducting excellent research in the field of cybersecurity. These ACEs-CSR are also active on accreditation.

Cyber Champions[35] is a not-for-profit organisation delivering an exciting community giveback initiative to promote best practices in digital literacy and online safety awareness to schools, youth organisations and interest groups across the UK. The programme is being driven by networks of Cyber Champions, young professional volunteers, supported by a growing number of private and public sector organisations motivated to make a difference to their local communities and up-skill future generations.

At a primary educational level, the *Cybersecurity Challenge UK*[36] creates learning and development opportunities that increase awareness of cybersecurity as a rewarding career and inspire more people to join the profession. The schools' programme is designed in partnership with teachers and employers, and the dedicated schools' programme offers lesson plans and supporting materials to help classes of 14–17-year-olds to make academic choices today that facilitate future entry into the sector.

While there is a large amount of education available, review participants were unsure if such offerings are needs-driven. Communication gaps between technical experts and C-level executives cause an inability for specific sectors to supply education providers with a list of necessary industry skills. The campaign "*Inspiring the future*"[37], an initiative supported by Bank of America (BOA UK), aims to bring together leading national bodies representing schools, colleges and employers on both cybersecurity and non-cyber issues.

There are outsourced providers of training in cybersecurity, and also private companies that are based internationally. These provide certification of qualifications such as the *Certified Information Systems Security Professional (CISSP)*[38], the *Certified Information Security Manager (CISM)*[39], *SANS*[40] *or CBEST*[41].

Public and private sector training exists collaboratively, is available locally, and is constantly adapting to the changing environment, as it seeks to build skillsets drawn from both sectors. Also government builds partnerships with other sectors, funds activity to train law enforcement, but not all members of staff are trained.

At this point, there is a lack of metrics to ensure that educational investments meet the needs of the cybersecurity environment. Moreover, it was identified that educational programmes do not necessarily align with practical cybersecurity and operational challenges and there are difficulties connecting the curriculum to the environment. In the private sector, stakeholders expressed their concern about the alignment of education and what the industry actually needs is an alignment that will require more long term evaluation.

We observe that there is a difference between education and skills. While there are cadres of experts that receive training in cybersecurity skills, this cadre is still too small to adequately meet the needs of the British society. As a result, at the moment there is a perceived skill

[35] http://cyberchampions.org/
[36] http://cybersecuritychallenge.org.uk/
[37] http://www.inspiringthefuture.org/about/test-child-of-about/
[38] http://www.cissp.com/
[39] http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx
[40] https://www.sans.org/
[41] http://crest-approved.org/industry-government/cbest/index.html

shortage, emphasising the need for combining education and practical training. Therefore, there is a need for more investment in cybersecurity and skill development programmes.

D3–2: National Development of Cybersecurity Education

This factor explores what kind of incentives structure exists for the national development of cybersecurity education: for example, whether any education strategy for developing cybersecurity skills exists; whether cybersecurity as a discipline is given priority in educational curricula; and whether adequate budget allocation is present.

Stage: Established

Public and private sector efforts exist to establish programmes for enhancing skills and capability in cybersecurity, while national education and skills priorities are informed by broad multi-stakeholder consultation. As mentioned above, the UK government has funded centres of excellence in cybersecurity, indicating that funding is dedicated to national research and education on cybersecurity. Also, government initiatives are directed towards increasing attractiveness of cybersecurity careers, but investment in these initiatives is expected to return more long-term benefits.

The private sector performs gap analysis regularly and it often shows that the market invests in cybersecurity practitioners. Such analyses indicate an increase of investment in cybersecurity education and skills development due to market needs. However, more investment and coordination of these programmes is needed in the UK.

Experts are being educated in cybersecurity, but it was noted during our consultation that there are not enough experts with a wide range of skills necessary for this field. Experts working in this field need to be more than IT professionals, enhancing skills such as the ability to understand security issues while building technology. As a result, at the moment there is a perceived skill shortage, emphasising the need for combining education and practical training. Additionally, there is a need to enhance the quality of training offerings by ensuring that those providing the training are well equipped. Training for these providers does not necessarily need to be cybersecurity specific, but has to be scoped and aligned according to their roles and responsibilities in regards to cybersecurity.

Cooperation and collaboration between stakeholders is enhanced and public-private partnerships exist. As mentioned above, both the public (such as the Cybersecurity Challenge UK) and the private sector (The Certified Information Systems Security Professional CISSP, the Certified Information Security Manager CISM, SANS or CBEST) continue their efforts to establish programmes for enhancing skills and capability in cybersecurity.

Cybersecurity skills, a guide for business (2014) [42] was developed in response to calls from businesses for an up-to-date and clear list of the key opportunities for them to engage with cybersecurity-specific skills and capability initiatives, particularly those that receive public funding. Initiatives supporting schools, vocational and higher education are reflected in this guide.

D3-3: Training and Educational Initiatives within the Public and Private Sector

Cybersecurity is a highly technical specialized field, and therefore strategic development and deployment of skillsets and tools to support those skillsets is central to maintaining organisations secure and mainstreaming cybersecurity culture within organisational structures. Apart from the question of strategic staffing, this factor reviews the scope of horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates to continuous skills development.

Stage: Established

For this factor there was a larger disparity among different stakeholders regarding the stage of maturity of the UK on training and educational initiatives within public and private sector. This disparity results in placing the UK at a *formative* or *strategic* stage due to the different initiatives and policies regarding training within the public and private sector.

Knowledge transfer from trained cybersecurity employees exists on an ad hoc basis and job creation initiatives for cybersecurity are established and encourage employers to train staff. While a training course in information protection is compulsory for all civil servants, it only provides basic level knowledge to public sector employees. Additionally, information security and data protection awareness is a part of the induction course that all staff must take on an annual basis. Spear phishing tests are conducted on members of staff, and there is a review and assessment of the tests. Despite these efforts, there is no central platform for sharing training information, nor joint requirements for cybersecurity training of the public and private sector, which will become necessary as large-scale cyber incidents are likely to involve both public and private organisations.

The Objective 4 of the UK's National Cyber Security Strategy is for the UK to have crosscutting knowledge, skills and capability it requires to deliver the wider Strategy. Through the National Cyber Security Programme (NCSP), the Department for Business Innovation and Skills (BIS), Government Communications Headquarters (GCHQ) and the Cabinet Office have partnered to lead and support activity to increase cybersecurity skills at all levels of education, and amongst the cybersecurity workforce. This work has been taken forward in close collaboration with business and the education and skills sectors.

The CESG Listed Advisor scheme (CLAS)[43] is another initiative of the UK government's National Technical Authority for Information Assurance (CESG). CLAS provides a pool of CESG Certified Professionals (CCPs) available to give Information Assurance (IA) advice or assistance to UK organisations. The CLAS partnership links the unique IA knowledge of CESG with the expertise

[42] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf
[43] http://www.cesg.gov.uk/servicecatalogue/CLAS/Pages/WhatisCLAS.aspx

and resources of a private sector network of nearly 700 CCPs. This initiative helps organisations that need IA consultants with specific IA expertise and CLAS is designed to help these organisations choose CLAS members with the expertise that best meets their needs.

As mentioned above there are structured cybersecurity training programs that specify precise roles and responsibilities. There are data systems, tools, and models available but the technical training is still required on how to operate these tools. The stakeholders from the public sector believed that simply making training available is not effective and that maybe training should be compulsory for all.

It was mentioned by stakeholders in the private sector that security in organisations depends on a limited number of experts. Moreover, it depends on individuals to transfer information to their colleagues. The finance sector was identified to be more advanced in this issue, since training is well established, and international exercises are being conducted within the context of information sharing, and thus some CNI companies can provide evidence of a dynamic stage of maturity for this consideration.

One example of this dynamic maturity is the C-BEST[44] initiative sponsored by CREST alongside the UK central Bank and the Bank of England (BoE). This initiative seeks to deliver controlled, bespoke, intelligence-led cybersecurity tests that replicate behaviours of those threat actors, assessed by government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. CBEST is the first initiative of its type to be led by any of the world's central banks. This initiative provided valuable information on lessons learned for future educational programmes.

The report "*Cybersecurity skills, business perspectives and government's next steps*" (2014)[45] highlighted a demand amongst businesses not only for more professionals with a range of technical skills, but also a demand for new entrants with stronger business skills and greater work experience. A range of reasoning for the skills shortage was suggested, including the immaturity of cybersecurity as a 'profession', low take-up of STEM (Science, Technology, Engineering and Maths) subjects, limited awareness of cybersecurity as an interesting and rewarding career at all levels of the education system. The report also highlighted the importance of increasing cybersecurity skills amongst those who create, purchase and use technology to reduce business vulnerability to cyberattack, and amongst company decision-makers who are responsible for managing business risks.

D3-4: Corporate Governance, Knowledge and Standards

This factor specifically looks into how private and state-owned companies', as represented by the highest executive level of senior management (C-level management), understand cybersecurity and react to changes related to the cybersecurity status quo.

Stage: Established

[44] http://crest-approved.org/industry-government/cbest/index.html

[45] CYBER SECURITY SKILLS, BUSINESS PERSPECTIVES AND GOVERNMENT'S NEXT STEPS, MARCH 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf

Boards and executives within private and state-owned companies have some awareness of cybersecurity issues and a general understanding of how companies are at risk, some of the primary methods of attack, and how their company deals with cybersecurity challenges (usually abdicated to the Chief Information Officer). However, in terms of event management, the majority of both the public and private sector is largely reactive.

During our consultation, various groups of stakeholders expressed different opinions regarding this issue depending on the sector they represented. Stakeholders from the finance sector claimed that the board sees cybersecurity as an operational risk and this is why it is now a higher priority. Moreover, the finance sector conducts exercises for contingency plans. Special training is provided to board members and managers. Board member understanding of cybersecurity is increasing and therefore there has been an increase in the signing off of investment in security.

Stakeholders from other areas of the private sector claimed that members of boards are not necessarily aware of cyber-risks, and usually avoid taking responsibility. The management and the capability of companies do not match the needs of those in a more operational role. Frequently, companies also do not reveal hacking incidents due to reputational harm.

The public sector, on the other hand, adopts a very different approach. Even if board members may not personally understand or recognise the need for a possible certification, they will be informed by advisors and may act on specific recommendations on steps to meet these needs.

As a result, there is a need to bridge the gap in risk perception and understanding, and consequences to the business or mission, which must partly be addressed by education of business leaders on cyber-risk, and partly by education of cyber professionals so that they can better understand the connection between cybersecurity controls and business harm reduction.

Recommendations

Following the information presented on the review of the maturity of Cybersecurity Education, Training and Skills, the Global Cyber Security Capacity Centre has developed the following set of recommendations.

There are education offerings in cybersecurity at the national and institutional level, ranging from primary to postgraduate levels. However, there is a concern that skills remain focused on the technical discipline whereas a multidisciplinary approach is required. The government promotes partnerships with various sectors in order to enhance education of employees, but still a large amount of employees are not trained. Additionally, there is a lack of metrics to ensure that educational investments meet the needs of the cybersecurity environment. In order to enhance the level of capacity regarding the availability of cybersecurity education and training we suggest the following:

- R3-1: Engrain information security training and education through all stages of education.
- R3-2: Allocate additional resources for the development of cybersecurity education and training programmes for public universities.

- R3-3: Develop partnerships for the development of interfaces to research and innovation through interaction between universities and the local economy. This way cybersecurity can keep pace with the changing environment.
- R3-4: Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, in order to enhance their expertise by combining education and practical training.
- R3-5: Create obligatory cybersecurity modules for students and teachers.
- R3-6: Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.
- R3-7: Expand the regular mandatory cybersecurity training for public sector staff to include training in issues such as data security and cybercrime and work into training all staff across all levels of central and local government.

Regarding the development of cybersecurity education, both public and private sector present efforts to establish programmes for enhancing skills and capability in cybersecurity, and these efforts are informed by broad multi-stakeholder consultation. Although there is a continuous increase of investment in cybersecurity education and skill development more investment and coordination of these programmes is needed in the UK. Additionally, experts working in this field need to enhance skills such as the ability to understand security issues while building technology. Therefore, we recommend the following:

- R3-8: Continue the efforts towards increasing attractiveness of cybersecurity careers, and promote cybersecurity as a 'profession' with clear career pathways.
- R3-9: Develop coordinated cybersecurity and skill development programmes to enhance skills, such as the ability to understand security issues while building technology, and ensure that the providers of the training are well equipped.
- R3-10: Enhance investment in cybersecurity and skill development programmes for combining education and practical training.

There are training and educational initiatives within the public and private sector. However, while a training course in information protection is compulsory for all civil servants, it only provides basic level knowledge to public sector employees. Within the private sector initiatives differ among different sectors. However, there is no central platform for sharing training information, nor requirements for cybersecurity training between the public and private sector. The following recommendations might enhance the capacity of training and educational initiatives:

- R3-11: Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools.
- R3-12: Develop a central platform for sharing training information for experts.
- R3-13: Create a national-level register of cyber-security experts.
- R3-14: Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.

The higher executive levels of senior management (C-level management) have an understanding of cybersecurity and react to changes to the cybersecurity landscape. Board-member understanding of cybersecurity is increasing due to an increase in investment on security. However, in terms of event management, the majority of both the public and private sector is largely reactive. There is a need to connect the technicians with the CEO's vision but also the technicians have to be able to talk with the CEOs and transfer the need for investment in cybersecurity. In summary, we recommend to:

- R3-15: Conduct cybersecurity trainings for public and private sector employees and board members, in a regular manner.
- R3-16: Promote cooperation and communication channels between cybersecurity professionals and business leaders to help build mutual understanding of cyber-risk and consequences for enterprise.

Dimension 4: Legal and Regulatory Frameworks

International experience attests to the crucial role legal and regulatory frameworks play in mainstreaming cybersecurity across sectors while presenting prevention, mitigation, and dispute mechanisms to individuals and organisations affected by cyber-threats. This dimension looks into the government's capacity to design and enact national legislation and accompanying by-laws directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, cybercrime, and on the stakeholder groups represented by law enforcement, prosecution services, and courts.

D4-1: Cybersecurity Legal Frameworks

This factor reviews availability and comprehensiveness of ICT security and privacy and data protection legislation, its relation to human rights legislation, as well as country's status in relation to regional and international treaties directly or indirectly related to cybersecurity.

Stage: Dynamic

Comprehensive ICT security legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in the UK**.** There are different pieces of legislation that speak to cybercrime. The *Computer Misuse Act 1990*[46], includes computer misuse offences such as a) unauthorised access to computer material; b) unauthorised access with intent to commit or facilitate commission of further offences; c) unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer. The Computer Misuse Act is currently under review.

Moreover, legislation provisions that apply to cybercrime offences are contained in broader legislation such as a) *the Forgery Act*[47] *1913, Art. 1; b) the Fraud Act*[48] *2006, Art. 1-8; c) the Protection of Children Act*[49] *1978, Art. 1; d) the Copyright, Designs and Patents Act*[50] *1988, Art. 1-8, Art. 56 and Art. 262.*

The *Human Rights Act*[51] 1998 (HRA) requires public bodies, like GCHQ, to protect citizens' rights under the European Convention on Human Rights.

The interception of communications operations are authorised under the *Regulation of Investigatory Powers Act 2000*[52] (RIPA). Warrants authorising interception can only be issued by a Secretary of State[53]. Before an interception warrant can be issued the Secretary of State must believe that a warrant is necessary on certain limited grounds and that the interception

[46] http://www.legislation.gov.uk/ukpga/1990/18/contents
[47] http://www.legislation.gov.uk/ukpga/1913/27/contents/enacted
[48] http://www.legislation.gov.uk/ukpga/2006/35/contents
[49] http://www.legislation.gov.uk/ukpga/1978/37/contents
[50] http://www.legislation.gov.uk/ukpga/1988/48/contents
[51] http://www.legislation.gov.uk/ukpga/1998/42/contents
[52] http://www.legislation.gov.uk/ukpga/2000/23/contents
[53] In the United Kingdom, a Secretary of State (SofS) is a Cabinet Minister in charge of a Government Department

is proportionate to what it seeks to achieve. These grounds are that interception is necessary: a) in the interests of national security; or b) in the interests of the economic well-being of the UK; or c) in support of the prevention or detection of serious crime. RIPA also requires safeguards to be in place to limit the use of intercepted material and related communications data. RIPA sets out the functions of two independent Commissioners, senior judges who have oversight of GCHQ's activities, the Interception of Communications Commissioner and the Intelligence Services Commissioner. GCHQ has a duty to cooperate with those Commissioners and to disclose all such documents and information they may require.

In 2011, the *European Framework on Electronic Communications* was implemented in the UK[54]. The Electronic Communications Framework[55] is the regulatory framework that applies to all transmission networks and services (including access) for electronic communications including: telecommunications (fixed and mobile); e-mail; access to the internet; and content related broadcasting. It consists of five Directives: the "Framework" directive (2002/21/EC); the "Access" directive (2002/19/EC); the "Authorisation" directive (2002/20/EC); the "Universal Service" directive (2002/22/EC); and the "E-Privacy" directive (2002/58/EC).

The Electronic Communications Act[56] 2000, chapter 7, is an Act to make provisions to facilitate the use of electronic communications and electronic data storage, to make provisions about the modification of Telecommunications licences granted under section 7 of the *Telecommunications Act*[57] 1984 and for connected purposes.

There are security standards but no national regulatory standards that companies have to adhere to in the UK. Each sector will have to follow different standards according to their needs and the threat they face. For this reason, it is difficult for the government to legislate these issues.

A comprehensive structure within the criminal justice system is in place to combat computer-related offences while respecting human rights and the country is engaged and works with international organisations on privacy and data protection. The UK has ratified international treaties, such as the European Convention on Human Rights (1998), and other agreements to adopt appropriate legislation, in order to combat criminal offences against privacy and data protection, by facilitating their detection, investigation, and prosecution.

The Crown Prosecution Service (CPS) has developed the *CPS Security and Information risk management policy*[58] 2013–2014. This policy aims to integrate information risk management into existing business and project risk as much as possible. Specific threats are managed via an ISO: 27001 assurance programme. Additional assessments of threats and their appropriate response are determined by the DSO, Chief Information Officer (CIO) and the departmental Senior Information Risk Officer (SIRO).

[54] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31567/10-1132-implementing-revised-electronic-communications-framework-consultation.pdf
[55] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf
[56] http://www.legislation.gov.uk/ukpga/2000/7/contents
[57] http://www.legislation.gov.uk/ukpga/1984/12/contents
[58] https://www.cps.gov.uk/publications/docs/systems/cps_security_and_information_risk_management_policy_0513.pdf

Information Assurance (IA) is a focus area of the Office of Cyber Security and Information Assurance (OCSIA) within the Cabinet Office. Information Assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data. It also ensures systems and processes used for those purposes are in line with the organisational policies. The Information Commissioner has the ability to impose fines on data controllers for security breaches and that results from the IA policy framework.

Regulation on the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information is contained in: a) *the Data Protection Act*[59] *1998; b) the Privacy and Electronic Communications (EC Directive) Regulations*[60] *2003; c) the Human Rights Act*[61] *1998; d) the Telecommunications (Data Protection and Privacy) Regulations*[62] *1999.*

Moreover, at a policy level, provisions regarding information assurance and data protection are contained in: a) *Data Handling Procedures in Government: Interim Progress Report*[63]*, December 2007; b) the Data Handling Procedures in Government: Cross Government Mandatory Minimum Measures*[64]*, December 2007; c) the Data Handling Procedures in Government: Final Report*[65]*, June 2008; d) the Data Handling in Government: The Scottish Government*[66]*, June 2008; e) Protecting Information in Government*[67]*, January 2010; f) Government Security Classifications April 2014*[68]*, October 2013; g) HMG Security Policy Framework*[69]*, April 2014; h) the Electronic Signatures Regulations 2002*[70] speak on electronic signatures and data protection.

During this review, stakeholders expressed the view that fostering cooperation at an international level and mutual legal assistance remains a challenge. International cooperation and mutual legal assistance in combating computer-related criminal offences is stronger at an EU level and weaker globally. There is no binding regulation on cooperation and sharing of information with the private sector and SMEs. There are voluntary schemes on this issue, such as CiSP, but there are no mandatory requirements that SMEs have to adhere to.

Substantive law in the UK speaks to cybercrime and the country has ratified regional and international instruments on cybercrime, such as the Budapest Convention[71], and

[59] http://www.legislation.gov.uk/ukpga/1998/29/contents
[60] http://www.legislation.gov.uk/uksi/2003/2426/regulation/2/made
[61] http://www.legislation.gov.uk/ukpga/1998/42/contents
[62] http://www.legislation.gov.uk/uksi/1999/2093/contents/made
[63] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60969/data_handling-interim_0.pdf
[64] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60968/cross-gov-actions.pdf
[65] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf
[66] http://www.gov.scot/Resource/Doc/229747/0062215.pdf
[67] http://webarchive.nationalarchives.gov.uk/20100304041448/http:/www.cabinetoffice.gov.uk/media/328380/protecting-information.pdf
[68] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
[69] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf
[70] http://www.legislation.gov.uk/uksi/2002/318/contents/made
[71] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/238194/8309.pdf

consistently seeks to implement these measures into domestic law. Cybercrime is in Tier 1 of the National Cybersecurity Strategy while the UK was one of the founders of the Joint Cyber Task Force (JCTF), which coordinates European action against cybercrime. Additionally, the UK collaborates with the United States of America and Interpol to combat cybercrime. The UK serves as an active contributor to global discourse on improving international cybercrime treaties while measures are in place to exceed minimal baselines specified in these treaties, which include procedures to amend substantive legal frameworks as required.

In the case of cross-border investigations, procedural law stipulates which actions need to be taken in particular cases, in order to successfully prosecute cybercrime. But, no specific law on cross-border investigation of cybercrime cases exists. *The Computer Misuse Act 1990* speaks to unauthorised access while the *Crime (International Co-operation) Act*[72] *2003* addresses the need to further cooperate with other countries in respect to criminal proceedings and investigations, to extend jurisdiction to deal with terrorist acts or threats outside the United Kingdom, to amend section 5 of the Forgery and Counterfeiting Act 1981 and make corresponding provision in relation to Scotland and for connected purposes.

In response to the Court of Justice of the EU ruling invalidating the Data Retention Directive in 2014, the UK Parliament passed *The Data Retention and Investigatory Powers Act*[73] *2014* to put data retention requirements on a firm statutory basis in national law.

D4–2: Legal Investigation

This factor studies the capacity of executive branch of government to prevent, combat, and investigate cyber incidents, attacks, and crimes, and of judiciary branch to prosecute cybercrime and electronic evidence cases. It also looks into the dynamic of formal and informal collaboration between different branches of government and between government and court system.

Stage: Strategic

A specialised National Cyber Crime Unit has developed strong capacity to investigate computer-related crimes, in accordance with domestic law; but "mainstreaming" of this capability to regional police services is less advanced. Law enforcement officers receive continuous training based on related responsibilities and new, evolving threat landscapes. They are able to utilise sophisticated digital forensic tools, and prosecute complex cybercrimes.

Domestic law enforcement agencies are informally integrated with regional and international police networks. In particular, the National Cyber Crime Unit (NCCU) is trained in cyber-investigation and has forensics capabilities, while the National Crime Agency also hosts the National Intelligence Hub that holds the national intelligence picture on cybercrime. The National Intelligence Hub organises meetings with the regional Units. This information then is collected and responsibilities are distributed and prioritised. At a local level, however, there are differences in the level of investigative capacity and skills, due to a lack of resources. Some

[72] http://www.legislation.gov.uk/ukpga/2003/32/contents
[73] http://www.legislation.gov.uk/ukpga/2014/27/contents

participants contended that existing legislation is sufficient for conducting investigations, while others indicated that new legislation is necessary to address challenges in cross border investigation.

Prosecutors receive training and have technological resources to prosecute cybercrime cases and those involving electronic evidence but these are not adequate. The Crown Prosecution Service (CPS)[74] at the national level is more advanced in prosecuting criminal cases investigated by the police than at a local level, and has dedicated prosecutors for cybercrime; however, some stakeholders felt basic training for prosecutors is not yet sufficient.

The judiciary receives training and there are resources to ensure prosecution of cybercrime and electronic evidence cases, but many stakeholders felt these efforts are not sufficient. The CPS is running a Scheme with the Court system in order to scale up training efforts in order to have the ability to present electronic evidence and to enhance infrastructure, but current efforts are not necessarily sufficient to provide adequate information and knowledge on prosecuting cybercrime. In order to overcome this challenge, there are formal collaboration mechanisms with multiple international counterparts and joint investigative teams at an EU level.

D4-3: Responsible Reporting

This factor explores if the public and private sectors enact a responsible disclosure policy and if there is sufficient capacity on part of both to continuously review and update this policy and synchronise it with recognised international responsible disclosure mechanisms. It also analyses existing capacity of stakeholders to receive, analyse, and disseminate vulnerability information gleaned through the responsible disclosure mechanisms.

Stage: Established

A vulnerability disclosure framework is in place, and there is ability to share technical details of vulnerabilities with other stakeholders who can distribute the information further. However, in the UK there is no compulsory incident reporting, and information disclosure remains voluntary.

The Cybersecurity Information Sharing Partnership (CiSP)[75], part of CERT-UK provides a safe platform for stakeholders and industry to share information on incidents. But, there is no regulation to oblige organisations or CNI companies to disclose information. The government also developed the "*Guiding Principles on Cyber Security: Guidance for Internet Service Providers* and Government"[76], which provides guidance on ISP-specific reporting mechanisms.

[74] http://www.cps.gov.uk/
[75] https://www.cert.gov.uk/cisp/
[76] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265328/bis-13-1327-guiding-principles-for-cyber-security-isps-and-hmg-FINAL.pdf

Recommendations

Following the information presented on the review of the maturity of legal and regulatory frameworks, the Global Cyber Security Capacity Centre has developed the following set of recommendations to be considered by the government. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

Comprehensive ICT security legislative and regulatory frameworks addressing cybersecurity have been implemented, and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in the UK**.** Moreover, legislation criminalises cybercrime offences. Regarding information sharing for the private sector and SMEs there are voluntary schemes on this issue, but no imposed regulation exists. The substantive and procedural law speak to cybercrime and prosecution procedures. Cybersecurity legal frameworks are characterised by a dynamic stage of maturity. In order for maturity to remain at such a high stage we recommend the following:

- R4-1: Enhance international cooperation and mutual legal assistance in combating online criminal offences.
- R4-2: Continue to push for stronger cybersecurity frameworks at the EU level and internationally.

Regarding investigative capacity, locally there are differences on the level of capacity and skills due to lack of resources. During this review, an issue raised by stakeholders was that there is limited capacity at the local law enforcement level to deal with cybercrime. Therefore, we recommend the following:

- R4-3: Strengthen national investigation capacity for computer-related crimes, with increased cooperation between the National Crime Agency and local police forces.
- R4-4: Expand and allocate funding on work in training law enforcement in understanding computer related crime in order to support investigations, especially at local level.
- R4-5: Enhance training and education of prosecutors and judges on computer related crimes.
- R4-6: Allocate additional resources to cybersecurity education & training for prosecutors and judges.
- R4-7: Introduce regular mandatory cybersecurity training for prosecutors and judges.
- R4-8: Enhance investigative capacity and skills locally.

A vulnerability disclosure framework is in place, and there is the ability to share technical details of vulnerabilities with other stakeholders who can distribute the information more broadly. However, in the UK there is no compulsory reporting. Regarding the issue, we recommend to:

- R4-9: Develop a responsible disclosure policy within public sector and facilitate its adoption in the private sector through targeted outreach, particularly in the CNI.
- R4-10: Encourage cybersecurity behaviour rather than imposing CNIs to adhere to certain frameworks on vulnerability disclosure.

Dimension 5: Standards, organisations, and technologies

This dimension brings forward the importance of implementation of cybersecurity standards and at least minimal acceptable practices; existence of well-functioning and high-capacity organisations coordinating cybersecurity with formal authority over multiple stakeholders; and the existence of a vibrant cybersecurity marketplace of technologies and cyber-insurance services.

D5-1: Adherence to Standards

This factor reviews government's capacity to design or adapt from other jurisdictions and implement cybersecurity standards and at least, minimal acceptable practices, especially those related to procurement procedures and software development. These standards and practices provide a minimum necessary baseline in the context of which strategic government decisions, especially organisational (resource) and financial (budgetary) decisions, should take place.

Stage: Established

Nationally agreed baseline of cybersecurity-related standards and minimal acceptable practices have been identified and adopted widely across the public sector and Critical National Infrastructure (CNI) organisations. Adoption and compliance is measured and reported, with adoption oversight from government – while the use of standards to mitigate CNI supply systems' risk is also considered.

Stakeholders informed us that the level of awareness of and implementation of standards depends on the scale of the industry. The major private-sector actors adopt standards and also adhere to government regulations. These standards differ in functionality; ISO: 27001 focuses on security processes, while other standards focus on control and risk management. The implementation of standards and minimal acceptable practices within CNI is at a more advanced stage of maturity. CNI adhere to 3GPP standards[77], while standards are adopted and resources are allocated according to thorough risk assessments. Sector-specific standards are being developed and implemented. The TI-EPF Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure[78] set guidelines to enhance maturity.

There is a wide spectrum of supply-chain standards adhered to, ranging from Cyber Essentials to ISO. SMEs often adhere to supply-chain standards, particularly the Cyber Essentials Scheme[79] and the Small Business Cyber Security Guidance[80]. The finance sector adheres to PCI SSC Data Security Standards which provide an actionable framework for developing a

[77] The term "3GPP specification" covers all GSM (including GPRS and EDGE), W-CDMA (including HSPA) and LTE (including LTE-Advanced) specifications. The following terms are also used to describe networks using the 3G specifications: UTRAN, UMTS (in Europe) and FOMA (in Japan).

[78] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61969/flu_tiepf_resilience_guidelines.pdf

[79] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

[80] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197177/bis13-780-small-business-cyber-security-guidance.pdf

robust payment-card data-security process, including prevention, detection and appropriate reaction to security incidents. The private sector seems to be more advanced and has a longer experience regarding implementation of standards than the public sector.

The government launched, in 2013, a guidance document "*A call for views and evidence: Cyber Security Organisational Standards*''[81] [82]. The aim of this document is to provide further guidance for stakeholders intending to submit evidence in support of an organisational standard and it provides acceptable criteria for Market Adoption / International Recognition, Organisational Outcomes, and Auditable Requirements.

While the evidence provided above highlight available security standards in the UK, these are not consistently adopted. Whether they will be adhered to depends on the organisation. The government does not necessarily impose adherence to standards on companies, but reputational harm as well as market demand does drive adoption of standards. There are few measurements available that seek to monitor the adoption of standards. During discussions, stakeholders agreed that organisational culture is very important and that boards need to be aware of the importance of cybersecurity standards so that they can select the appropriate standards to their needs.

The implementation of standards in procurement practices meets international IT and security guidelines, standards and acceptable practices and is evidenced through measurement and quality assessments of process effectiveness. Critical aspects of procurement such as prices and costs, quality, timescales and other value-added activities are continuously improved in the context of wider resource-planning across enterprises, and there is also an ability to adapt to changes.

The extent of the implementation of standards in procurement depends on the sector and whether that sector adopts a reactive or a proactive approach. The government follows a classification scheme: across government there are standards for procurement, which maintain a strict patching requirement. The private sector also conducts risk assessments and these drive the adoption of procurement standards. It was noted that cyber-threats can derive from engaging agencies regarding procurement across the supply chain matrix, not just from technology per se. Telecommunication providers offer a wide range of services and often adhere to standards tailored to their specific objectives. Adherence to standards is frequently reviewed according to needs.

Methodologies for software-development processes that focus on integrity and resilience are being discussed and promoted by the UK government and professional communities. Evidence exists of organisations within the CNI and the public sector supplying or seeking to adopt standards in code development, and achieving some accreditations with government promotion of secure practices. As mentioned above with regards to implementation of standards for procurement, differences also exist in the adoption of standards for software development. Within government the degree of implementation of standards depends on the severity and importance of the functions carried out by the respective department of the

[81] https://stewartroom.co.uk/wp-content/uploads/2014/06/UK-Cyber-Security-Cyber-Security-Organisational-Standards-Guidance-April–2013.pdf

[82] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf

government. An area of interest at the moment is security-by-design, combining the principles of software design with the principles of security.

The elevated cost of standard-implementation and of secure software development makes achieving a higher stage of maturity in this factor difficult for some government ministries and organisations.

D5–2: National Infrastructure Resilience

This factor reviews how effectively the government deploys and manages infrastructure technologies (own government networks and systems) and how it performs monitoring and evaluation of the costs for infrastructure technologies and their resilience. In addition, it looks into existence and exercise of government's capacity to engage in strategic planning and maintain sufficient scientific, technical, industrial, and human capabilities.

Stage: Established

Technology and processes deployed meet international IT standards, guidelines and best practices. Use of the Internet for communication between all stakeholders is integrated into everyday operating practice while the internet is widely used for business, e-commerce and electronic transactions. Also, authentication processes and measures are established. Most organisations follow standards and processes such as authentication, but most of these are primarily focused on infrastructure protection. There are security processes in place, and many organisations conduct threat assessments and have established risk-management processes. However, these processes have not yet reached an advanced level. There seems to be no business model implemented on a large scale to measure impact. The cost-benefit discussion is framed by customer breach rather than advanced knowledge of the threat landscape. It becomes an insurance policy, rather than a business-policy proposition.

CNI organisations have established security processes across private and public sector especially for security risk management, threat assessment, and incident response and business continuity. CNI organisations are more advanced since they have strategic planning and service continuity processes in place, and their scientific, technical, industrial and human capabilities are being systematically maintained, enhanced and perpetuated in order to maintain their resilience.

Risk-based management and best practices with formal vulnerability analysis is conducted and assessments of national resilience for CNI and essential services are conducted to protect information systems of the country and the operators of CNI and essential services. National infrastructure is managed, but the national resilience is not documented. Moreover, the government often contracts CNIs, so consequently resilience is built through these contracts. CERT-UK has an independent relationship with Telecommunication partners and has established processes for response.

The Centre for the Protection of National Infrastructure (CPNI) provides a range of guidance documents and technical notes[83] aimed at improving practices and raising awareness of current issues related to information security. These cover varied topics such as threats,

[83] http://www.cpni.gov.uk/advice/cyber/

security on mobile devices, SCADA (Supervisory Control and Data Acquisition) systems, password advice and incident recovery. There is also a link to the "*20 Critical Security Controls*[84]", which provides a baseline for basic security measures that any organisation should adopt to improve its cybersecurity posture.

D5-3: Cybersecurity Marketplace

This factor studies the availability of competitive cybersecurity technologies and their strategic deployment and maintenance by public and private sectors. It also reviews the state of cyber-insurance marketplace and its offerings through the study of perception of financial risks by public and private sectors and perceived demand for cybercrime insurance.

Stage: Established

In this factor there are two main issues that we are looking at, a) cybersecurity technologies and b) cyber-insurance marketplace. After reviewing both aspects of this factor we have identified quite a large disparity between them. We need to acknowledge that cybersecurity technologies reach *a dynamic stage* of maturity, while cyber-insurance market is at a *formative stage*. This is why we need to present these two issues separately. This factor is characterised at an established stage in an effort to combine both results.

Stage: Dynamic

Cybersecurity technologies, including software, abide by secure coding guidelines, best practices and adhere to internationally recognised standards. Security technologies and processes across sectors are up-to-date, based on strategic risk assessment. Risk assessments also inform the application of market incentives toward prioritised products to mitigate identified risks.

Additionally, core development activities including configuration and document management, security development and lifecycle planning of software have been adopted. Many organisations also collaborate in order to conduct research and produce threat analytics. While British technologies are prolific, the country's marketplace is not independent but relies on other countries for technology as well. During this review, stakeholders referred to examples of domestic cybersecurity products, which are exported to other nations and are considered superior products.

Stage: Formative

The need for a market in cybercrime insurance has been identified through the assessment of financial risks for public and private sector. Sharing of best practices in assessment and risk reduction, including the development and use of appropriate standards and varied products is now being discussed.

Although cybercrime insurance is available, it is described as immature because there are no established best practices and there are significant areas where insurance is not offered. Also a lack of sharing of incidents inhibits the collection of data and makes it harder for insurance companies to estimate the cost of cyber-impact. Insurance companies are driven my macro

[84] http://www.cpni.gov.uk/advice/cyber/Critical-controls/

rather than micro trends. They cover various risks, especially those related to data breaches, but losses due to reputational harm and the theft of intellectual property can hardly be evaluated even qualitatively at the moment.

Stakeholders from the private sector raised the issue that the size of the company matters, and that SMEs do not pay much attention to this matter. At the SME level there is a discussion on cyber-insurance, and especially data protection insurance. Additionally, the finance sector is considering insurance of data.

The report *"UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk"*[85] focuses on how insurance companies can help make UK companies more resilient to the cyber-threat, and is the result of cooperation between representatives of the UK government and the insurance industry, led by the Cabinet Office and Marsh[86]. This report addresses three themes and offers up recommendations for each: a) helping firms get to grips with cyber-risk; b) helping the insurance industry to establish cyber-insurance as part of firms' cybersecurity toolkits; c) helping London to become a global centre for cyber-risk management.

Recommendations

Following the information presented on the review of the maturity of standards, organisations, and technologies, the Global Cyber Security Capacity Centre has developed the following set of recommendations to be considered by the government. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model.

Although international standards and best practises are adopted widely across the public sector and Critical National Infrastructure (CNI) organisations the level of awareness and implementation of ICT standards and standards in procurement depends on the scale of industry. Additionally, the elevated cost of the implementation of standards and of secure software development makes achieving a higher stage of maturity in this factor difficult for some government ministries and organisations. Therefore, we recommend the following:

- R5-1: Establish a programme to strengthen government's capacity to adapt or adopt international standards to all scales of industry.
- R5-2: Promote the adoption of international standards within the public sector.
- R5-3: Promote awareness and implementation of standards among SMEs.
- R5-4: Incorporate cybersecurity considerations in all stages of software and system development and processes.
- R5-5: Adopt core development activities including configuration and document management, security development and lifecycle planning of software.
- R5-6: Establish a process to measure the impact of standard adoption.

[85] https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html
[86] https://www.marsh.com/uk/about-marsh/about-us.html

- R5-7: Conduct risk assessment exercises in order to inform adherence to selected standards.
- R5-8: Embed security-by-design, in testing software.

Regarding national infrastructure resilience, technology and processes deployed meet international IT standards, guidelines and best practices. But, these processes have not reached a rigorous level for security risk management, threat assessment, incident response and business continuity. Moreover, there seems to be no business model implemented in a large scale to measure impact. In order for the maturity of national infrastructure resilience to enhance we recommend the following:

- R5-9: Enhance the level of security processes in place (threat assessments and risk management processes).
- R5-10: Document national resilience.
- R5-11: Establish high-level security processes across private and government sectors especially for security risk management, threat assessment, incident response and business continuity.
- R5-12: Conduct regular assessments of processes and national information infrastructure security according to standards and guidelines.
- R5-13: Conduct assessments of national resilience for CNI and essential services to protect information systems of the country and the operators of CNI and essential services.
- R5-14: Develop metrics to assess benefits for businesses from additional investments in technology.
- R5-15: Invest in ICT research and cooperation between academia, research and industry to strengthen the software-engineering competencies of domestic ICT companies.
- R5-16: Update security features in software architecture.
- R5-17: Develop automated security functions in software and computer system configuration.

The last issues we reviewed in the concept of cybersecurity marketplace are cybersecurity technologies and cyber-insurance marketplace. In the UK there are examples of domestic cybersecurity products. However, domestic capacity is not at such an enhanced level as to eliminate national dependence on foreign technologies. Additionally, although the need for a market in cybercrime insurance has been identified through the assessment of financial risks for public and private sector, this market is described as an immature business because of the lack of best practices in the field. We recommend the following:

- R5-18: Promote sharing of information and best practices among organisations, to enhance covering of cybercrime insurance.
- R5-19: Select coverage of cybercrime insurance based on strategic planning needs and identified risk.
- R5-20: Consider the deployment of a government-backed cyber-reinsurance market.

Additional Reflections

It must be remarked that the level of participation in the review by stakeholders was lower than we might have hoped for, and that not all stakeholder groups were represented (notably the Intelligence and Defence Communities). This necessarily limits the comprehensiveness of the results and necessitates more reliance, in some areas, on desk research.

This was the ninth country review that we have supported directly, and the first of an *advanced* nation. As such, it visited a number of previously unexplored corners of the model and provided useful input into the evolution of the model. We note that participants generally (and commendably) refrained from stretching to claim higher levels of maturity than could be evidenced, and so we are confident that the assessments ultimately made are sound and possibly conservative.

We understand that the UK is in the process of developing different aspects of cybersecurity capacity including (but not limited to) revision of the National Cybersecurity Strategy, and that the UK aims at continuous engagement in international cooperation. These efforts will set the foundations for an advanced capacity in the future. We hope that this review will offer useful insight to the UK and that our recommendations on how to increase cybersecurity capacity will contribute to the on-going work on the development of the UK National Cybersecurity Strategy 2016–2020.

Appendix I

Table I: Review Results

Dimension	Capacity Factor	Stage of Maturity	Brief Description	Links
Dimension 1 Cyber Security Policy and Strategy	**D1-1 National Cybersecurity Strategy**	**Strategic**	The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world (CSS) The content of the national cybersecurity strategy is updated based on results of the application of metrics. The government is now in the process of revising the national cybersecurity strategy (2015–2020), based on threats, lessons learned and the outcomes of the strategy implementation.	The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386094/Infographic_The_UK_Cyber_Security_Strategy_December_2014.pdf Annual Report – CERT-UK https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf
	D1–2 Incident Response	**Established**	A central registry of national-level cyber-incidents is established and held by CERT-UK. CERT-UK performs exercises, provides advice to entities and directs them to the Council of Registered Ethical Security Testers (CREST).	https://www.cert.gov.uk/ https://www.cert.gov.uk/cisp/ Cabinet Office, Responding to Emergencies: The UK Central Government Response: Concept of Operations, 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192425/CONOPs_incl_revised_chapter_24_Apr-13.pdf Emergency Response and Recovery Non statutory

				guidance accompanying the Civil Contingencies Act 2004 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/253488/Emergency_Response_and_Recovery_5th_edition_October_2013.pdf Cabinet Office, Civil Contingencies Secretariat. The Lead Government Department and its role – Guidance and Best Practice https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61355/lead-government-departments-role.pdf
	D1-3 Critical National Infrastructure	**Established**	There is a list of identified critical national infrastructure assets. The Treasury keeps a list of CNI assets, which is reviewed on an annual basis. The Centre for the Protection of Critical Infrastructure (CPNI) defines reporting requirements. Risk management and security measures and guidelines for CNI cybersecurity best practice have been established.	http://www.cpni.gov.uk/ http://itlaw.wikia.com/wiki/Telecommunications_Industry_Security_Advisory_Council
	D1-4 Crisis Management	**Established**	Cybersecurity exercises are conducted. CERT-UK holds the exercise plan and more sophisticated exercises are planned for subsequent years.	
	D1-5 Cyber Defence Consideration	**Established**	There is no discrete Cyber Defence Strategy in the UK. However, through the Cyber Programme, the SDSR and the NSS are being used for this purpose. SDSR and NSS 2015 were published in November 2015, after completion of the evidence-gathering for this review. The University Short Course Programme (USCP) forms part of the wider strategy of the Services to contribute to the improvement of the general education of Service personnel. USCP provides personnel	https://www.gov.uk/government/organisations/joint-forces-command/about https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_da

			the opportunity to address matters of current importance and research and development, such as cybersecurity, within an academic environment. The Army Reserve provides support to the Regular Army at home and overseas, provides highly trained soldiers who can work alongside the Regulars on missions in the UK and overseas. The Joint Cyber Reserve will be an essential part of ensuring defence of national security in cyberspace and protection of vital computer systems and capabilities.	ta/file/62482/strategic-defence-security-review.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf Achieving the strategic edge through people: 2040 https://www.gov.uk/government/news/achieving-the-strategic-edge-through-people–2040 The University Short Course Programme http://www.army.mod.uk/documents/general/20150625-ShortCourseProspectus-PRINT-O.pdf#search=cyber war The Army Reserveshttp://www.army.mod.uk/reserve/31781.aspx Joint Cyber Reserve https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit
	D1-6 Digital Redundancy	**Established**	In the UK, emergency response asset priorities and standard operating procedures are established in the event of a communications disruption. The Department for Culture, Media and Sport is responsible for the resilience of the communication sector.	
Dimension 2 Cyber Culture and Society	**D2-1 Cybersecurity Mind-Set**	**Formative**	Within the government, the private sector and society at large the cybersecurity mind-set is reactive rather that proactive. Every government department has been briefed on the “10 Steps to Cyber Security”, they have been informed on the threats; the language of cybersecurity is also being embedded	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

			in all departments.	
	D2– 2Cybersecurity Awareness	**Established**	The national coordinated cybersecurity campaign "Cyber Streetwise" is a joint departmental initiative which attempts to drive behavioural change by providing tips and advice on improving online security. The campaign targets both home users and businesses. "Cyber Essentials" is a coordinated government-backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. The "GetSafeOnline Campaign" focuses on users at home and businesses. The "Webwise Campaign" focuses mainly on parents and home users.	www.cyberstreetwise.com http://www.cyberstreetwise.com/cyberessentials/?&nginxId=263c74e8-f8c9-45e1-c5e2-c51e4e1dd520 www.getsafeonline.org http://www.bbc.co.uk/webwise/0/
	D2-3 Confidence and trust on the Internet	**Formative**	Companies have made a significant effort to shift their services online, but there is no coordinated programme for trust building. E-government services are being used widely in the UK with recognition of the need for the application of security measures to promote trust in e-services. However, there is no coordinated programme to promote trust in e-government services. E-commerce services are fully established in a secure environment, while multiple stakeholders continue to invest in e-commerce.	Dutton, W. H., and Shepherd, A., (2005) 'Confidence and Risk on the Internet', pp. 207-44 in R. Mansell and B. S. Collins (eds) Trust and Crime in Information Societies, Cheltenham: Edward Elgar Publishing.
	D2-4 Privacy Online	**Established**	The government adheres to regionally and internationally recognised standards for human rights, in relation to privacy. The Information Commissioner's Office (ICO) was set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Interception of Communications Commissioner's Office (IOCCO) is responsible for keeping under review the interception of communications and the acquisition and disclosure of	https://ico.org.uk http://www.iocco-uk.info/default.asp

			communications data.	
Dimension 3 Cybersecurity Education, Training and Skills	**D3-1 National Availability of Cybersecurity Education and Training**	**Established**	The launch of Government Communications Headquarters (GCHQ) online training available to all indicates the interest in cybersecurity education. GCHQ and the Engineering and Physical Sciences Research Council (EPSRC) have set up a scheme to recognise Academic Centres of Excellence in Cyber Security Research (ACEs-CSR). At a primary education level, the 'Cybersecurity Challenge UK' creates learning and development opportunities that increase awareness of cybersecurity as a rewarding career and inspire more people to join the profession. There are outsourced providers of training in cybersecurity. These provide also certification such as The Certified Information Systems Security Professional (CISSP), the Certified Information Security Manager (CISM), System Administration, Networking, and Security Institute (SANS) or Central Bank Ethical Security Testers (CBEST).	http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-certifies-Masters-Degrees-in-Cyber-Security.aspx http://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/296010/bis-14-660-developing-our-capability-in-cyber-security-academic-centres-of-excellence-in-cyber-security-research.pdf http://cybersecuritychallenge.org.uk/ http://www.cissp.com/ http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx https://www.sans.org/ http://crest-approved.org/industry-government/cbest/index.html
	D3–2 National development of cybersecurity education	**Established**	Public and private sector efforts exist to establish programmes for enhancing skills and capability in cybersecurity. "*Cybersecurity skills, a guide for business*" (2014) was developed in response to calls from businesses for an up-to-date and clear list of the key opportunities for them to engage with cybersecurity-specific skills and capability initiatives, particularly those	"Cybersecurity skills, a guide for business" (2014) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf

			that receive public funding. Initiatives supporting schools, vocational and higher education are reflected in this guide.	
	D3-3 Training and educational initiatives within public and private sector	**Established**	Through the National Cyber Security Programme (NCSP) the Department for Business Innovation and Skills (BIS), Government Communications Headquarters (GCHQ) and the Cabinet Office have partnered to lead and support activity to increase cybersecurity skills at all levels of education, and amongst the cybersecurity workforce. The Communications-Electronics Security Group (CESG) Listed Advisor scheme (CLAS) is another initiative of the UK government's National Technical Authority for Information Assurance. "Cybersecurity skills, a guide for business" (2014) was developed in response to calls from businesses for a current and clear listing of the key opportunities for them to engage with cybersecurity skills and capability initiatives.	http://www.cesg.gov.uk/servicecatalogue/CLAS/Pages/WhatisCLAS.aspx https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386248/bis-14-1276-cyber-security-skills-a-guide-for-business.pdf
	D3-4 Corporate Governance, Knowledge and Standards	**Established**	Boards and executives within private and state-owned companies have some awareness of cybersecurity issues and an understanding of how companies are at risk in general. However, regarding event management both the public and private sector is largely reactive.	
Dimension 4 Legal and Regulatory Frameworks	**D4-1 Cybersecurity Legal Frameworks**	**Dynamic**	The Computer Misuse Act 1990, includes computer misuse offences such as a) unauthorised access to computer material; b) unauthorised access with intent to commit or facilitate commission of further offences; c) unauthorised acts with intent to impair, or with recklessness as to impairing operations of computers. Legislation regarding cybercrime offences includes a) the Forgery Act 1913, Art. 1; b) the Fraud Act 2006, Art. 1-8; c) the Protection of Children	http://www.legislation.gov.uk/ukpga/1990/18/contents http://www.legislation.gov.uk/ukpga/1913/27/contents/enacted http://www.legislation.gov.uk/ukpga/2006/35/contents http://www.legislation.gov.uk/ukpga/1978/37/contents

			Act 1978, Art. 1; d) the Copyright, Designs and Patents Act 1988, Art. 1-8, Art. 56 and Art. 262. The Human Rights Act 1998 (HRA) requires all public bodies to comply with the European Convention on Human Rights. The interception of communications operations is authorised under the Regulation of Investigatory Powers Act 2000 (RIPA). The Electronic Communications Act 2000, chapter 7, makes provision for the use of electronic communications and electronic data storage. The Electronic Communications Act 2000, chapter 7, is an Act to make a provision to facilitate the use of electronic communications and electronic data storage. In 2011, the European Framework on Electronic Communications was implemented in the UK. The Crown Prosecution Service (CPS) has developed the CPS Security and Information risk management policy 2013 – 2014. CPS policy aims to integrate information risk management into existing business and project risk as far as possible. Regulation on the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information include: a) the Data Protection Act 1998; b) the Privacy and Electronic Communications (EC Directive) Regulations 2003; c) the Human Rights Act 1998; d) The Telecommunications (Data Protection and Privacy) Regulations 1999; e) Telecommunications (Data Protection and Privacy) (Amendment) Regulations 2000(2). Legislation regarding information assurance and data protection include:	http://www.legislation.gov.uk/ukpga/1988/48/contents http://www.legislation.gov.uk/ukpga/1998/42/contents http://www.legislation.gov.uk/ukpga/2000/23/contents http://www.legislation.gov.uk/ukpga/2000/7/contents The Electronic Communications Framework https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31567/10-1132-implementing-revised-electronic-communications-framework-consultation.pdf https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf https://www.cps.gov.uk/publications/docs/systems/cps_security_and_information_risk_management_policy_0513.pdf http://www.legislation.gov.uk/ukpga/1998/29/contents http://www.legislation.gov.uk/uksi/2003/2426/regulation/2/made http://www.legislation.g

			a) Data Handling Procedures in Government: Interim Progress Report , December 2007; b) the Data Handling Procedures in Government: Cross Government Mandatory Minimum Measures , December 2007; c) the Data Handling Procedures in Government: Final Report , June 2008; d) the Data Handling in Government: The Scottish Government , June 2008; e) Protecting Information in Government , January 2010; f) Government Security Classifications April 2014 , October 2013; g) HMG Security Policy Framework , April 2014; h) the Electronic Signatures Regulations 2002 speak on electronic signatures and data protection. The UK has ratified the Budapest Convention in Cybercrime in 2011.	ov.uk/ukpga/1998/42/contents http://www.legislation.gov.uk/uksi/1999/2093/contents/made https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60969/data_handling-interim_0.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60968/cross-gov-actions.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf http://www.gov.scot/Resource/Doc/229747/0062215.pdf http://webarchive.nationalarchives.gov.uk/20100304041448/http:/www.cabinetoffice.gov.uk/media/328380/protecting-information.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

				http://www.legislation.gov.uk/uksi/2002/318/contents/made The Budapest Convention in Cybercrime https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/238194/8309.pdf
	D4–2Legal investigation	**Strategic**	Law enforcement officers receive continuous training based on relative responsibilities and new, evolving threat landscapes and are able to use sophisticated digital forensic tools. Prosecutors and the Judiciary receive training and have some resources to ensure effective and efficient prosecution of cybercrime and electronic evidence cases. The Crime (International Co-operation) Act 2003 speaks on furthering co-operation with other countries in respect of criminal proceedings and investigations. The Data Retention and Investigatory Powers Act 2014 makes provisions, in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, for the retention of certain communications data.	http://www.legislation.gov.uk/ukpga/2003/32/contents http://www.legislation.gov.uk/ukpga/2014/27/contents
	D4-3 Responsible Reporting	**Formative**	In the UK there is no compulsory reporting; rather, information disclosure remains voluntary. The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015 (Emergency alerts 16A) speaks on reporting obligations for public communications providers, for the purpose of providing an emergency alert service, disregard the restrictions on the processing of data relating to users or subscribers. The government also developed the "Guiding Principles on Cyber Security: Guidance for Internet Service	http://www.legislation.gov.uk/uksi/2015/355/pdfs/uksi_20150355_en.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265328/bis-13-1327-guiding-principles-for-cyber-security-isps-and-hmg-FINAL.pdf

			Providers and Government" referring to reporting mechanisms.	
Dimension 5 Standards, organisations, and technologies	**D5-1 Adherence to standards**	**Established**	There are recommended standards on ICT, on procurement and software development. The implementation of these standards is voluntary. Different standards such as ISO: 27001 on processes, but also standards focused on control and risk management are followed by the majority of organisations. CNI adhere to 3rd Generation Partnership Project (3GPP) standards. SMEs adhere to standards and the Cyber Essentials Scheme and the Small Business Cyber Security Guidance In 2013, the government launched a guidance document "A call for views and evidence: Cyber Security Organisational Standards".	https://stewartroom.co.uk/wp-content/uploads/2014/07/UK-Cyber-Security-Cyber-Essentials-Requirements-June–2014.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197177/bis13-780-small-business-cyber-security-guidance.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf
	D5–2National Infrastructure Resilience	**Established**	Technology and processes deployed meet international IT standards, guidelines and best practices. The Centre for the Protection of National Infrastructure (CPNI) provides a range of guidance documents and technical notes aimed at improving practices and raising awareness of current issues related to information security. These cover such varied topics as threats, security on mobile devices, SCADA (Supervisory Control and Data Acquisition) systems, password advice and incident recovery. There is also a link to the "20 Critical Security Controls", which provides a	http://www.cpni.gov.uk/advice/cyber/ http://www.cpni.gov.uk/advice/cyber/Critical-controls/

			baseline of basic security measures that any organisation should take to improve its cybersecurity posture.	
	D5-3 Cybersecurity Marketplace	**Established**	Cybersecurity technologies, including software, abide by secure coding guidelines, best practices and adhere to internationally recognised standards. The need for a market in cybercrime insurance has been identified through the assessment of financial risks for public and private sector. The report "UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk" focuses on how insurance can help make UK companies more resilient to cyber-threat, and is the result of co-operation between representatives of the UK Government and the insurance industry, led by the Cabinet Office and Marsh.	https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html

Appendix II

Table II: Recommendations

Dimension	Capacity Factor	Current Stage of Maturity	Recommendations to Enhance Stage of Maturity
Dimension 1 Cyber Security Policy and Strategy	**D1-1 National Cybersecurity Strategy**	**Strategic**	• **R1-1:** Develop the capability to modify the content of the strategy in response to the cybersecurity environment regularly and incorporate it in the strategic plan. • **R1-2:** Encourage a broader conversation with all stakeholders including the private sector, wider society and international partners during the yearly review of the National Cyber Security Programme (NCSP). • **R1-3:** Set a mechanism in place to implement the strategy in full scope, including at a local level. • **R1-4:** Enhance the capacity for adapting focus on incident identification and analysis in response to environmental changes. • **R1-5:** Develop predictive methods to assess risk, its propagation and its aggregation for the National and CNI lens.
	D1–2 Incident Response	**Established**	• **R1-6:** Incorporate an early warning capacity into the mission of the emergency response organisation. • **R1-7:** Embed tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities in emergency response organisation(s). • **R1-8:** Prioritise multi-level national coordination between all levels and sectors to incident response at regional and international level. • **R1-9:** Prioritise drafting regulations on incident response, and promoting reporting of incidents. • **R1-10:** Appoint a mandate authority to ensure reporting of incidents. • **R1-11:** Develop a mechanism of capturing incidents on lower governmental levels, locally.
	D1-3 Critical National Infrastructure	**Established**	• **R1-12:** Develop a mechanism of asset analysis on lower governmental levels, locally. • **R1-13:** Prioritise listing of CNI assets and regularly re-appraise to capture changes in the threat environment. • **R1-14:** Invest in capability of Board Members and Senior Leaders of organisations to understand cyber-risk intelligence, so that they can lead in the face of crisis and take their part in risk management more generally. • **R1-15:** Implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio. • **R1-16:** Strengthen formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector.

			• **R1-17:** Execute procedures to optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations as needed to encompass incident prevention, detection and response.
	D1-4 Crisis Management	**Established**	• **R1-18:** Prioritise crisis management exercises, especially at a local level, and communicate the value of the exercises. • **R1-19:** Conduct compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises to inform strategic investment in future emergency response assets.
	D1-5 Cyber Defence Consideration	**Established**	• **R1-20:** Draft a Cyber Defence Strategy. • **R1-21:** Enhance funding efforts for research and development focused on automated cyber-defence response systems, and speed up time to operational impact. Consider developing a performance assessment environment for assessing performance of methods in a non-classified environment, to support procurement and on-going requirements development. • **R1-22:** Conduct constant review of the evolving threat landscape in cybersecurity to ensure that cyber-defence policies continue to meet national security objectives. • **R1-23:** Prioritise compliance of the National Security Strategy and National Strategic Defence and Security Review with international law and consistency with national and international rules of engagement in cyberspace.
	D1-6 Digital Redundancy	**Established**	• **R1-24:** Enhance cooperation between public and private sector in cyber-specific work and specifically digital and non-digital systems redundancy. • **R1-25:** Communications and emergency response assets need to have both non-digital network backups and access to personnel trained to activate and maintain them.
Dimension 2 Cyber Culture and Society	**D2-1 Cybersecurity Mind-Set**	**Formative**	• **R2-1:** Enhance efforts at all levels of government to promote understanding of risks and threats, but also the design of systems that enable users across society to easily embed secure practices into their everyday use of the Internet and online services. • **R2-2:** Promote sharing of information on incidents and best practices among organisations to promote a proactive cybersecurity mind-set. • **R2-3:** Promote prioritisation of risk and threat understanding for SMEs.
	D2–2Cybersecurity Awareness	**Established**	• **R2-4:** Maintain and expand the existing awareness programmes to cover various target groups (such as children, parents, experts, SMEs, government agencies) linked to the national cybersecurity strategy. • **R2-5:** Enact evaluation measurements to study effectiveness of the awareness programmes at a level

			where they inform future campaigns taking into account gaps or failures. • **R2-6:** Promote awareness of risks and threats at lower levels of the government. • **R2-7:** Promote a high level of multi-stakeholder engagement in the design of awareness campaigns. • **R2-8:** Encourage the private sector to provide awareness education.
	D2-3 Confidence and trust on the Internet	**Formative**	• **R2-9:** Promote trust in e-government and e-commerce services through regulation ensuring personal data privacy and adherence of e-government services to the highest cybersecurity protection standards. • **R2-10:** Develop a feedback mechanism to provide evidence on trust in e-government and e-commerce services, while helping users to understand the complex relationships between trust and use of the Internet.
	D2-4 Privacy Online	**Established**	• **R2-11:** Promote understanding and implementation of privacy standards and policies within local government. • **R2-12:** Sensitise employees on their privacy rights and obligations within the organisation. • **R2-13:** Sensitise all sectors of the public to privacy and data protection issues, including youth but also other vulnerable groups.
Dimension 3 Cybersecurity Education, Training and Skills	**D3-1 National Availability of Cybersecurity Education and Training**	**Established**	• **R3-1:** Engrain information security training and education through all stages of education. • **R3-2:** Allocate additional resources for the development of cybersecurity education and training programmes for public universities. • **R3-3:** Develop partnerships for the development of interfaces to research and innovation through interaction between universities and the local economy. This way cybersecurity can keep pace with the changing environment. • **R3-4:** Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, in order to enhance their expertise by combining education and practical training. • **R3-5:** Create obligatory cybersecurity modules for students and teachers. • **R3-6:** Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment. • **R3-7:** Expand the regular mandatory cybersecurity training for public sector staff to include training in issues such as data security and cybercrime and work into training all staff across all levels of central and local government.
	D3–2 National development of	**Established**	• **R3-8:** Continue the efforts towards increasing attractiveness of cybersecurity careers, and promote cybersecurity as a ‘profession’ with clear career pathways.

	cybersecurity education		• **R3-9:** Develop coordinated cybersecurity and skill development programmes to enhance skills, such as the ability to understand security issues while building technology, and ensure that the providers of the training are well equipped. • **R3-10:** Enhance investment in cybersecurity and skill development programmes for combining education and practical training.
	D3-3 Training and educational initiatives within public and private sector	**Established**	• **R3-11:** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools. • **R3-12:** Develop a central platform for sharing training information for experts. • **R3-13:** Create a national-level register of cyber-security experts. • **R3-14:** Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.
	D3-4 Corporate Governance, Knowledge and Standards	**Established**	• **R3-15:** Conduct cybersecurity trainings for public and private sector employees and board members, in a regular manner. • **R3-16:** Promote cooperation and communication channels between cybersecurity professionals and business leaders to help build mutual understanding of cyber-risk and consequences for enterprise.
Dimension 4 Legal and Regulatory Frameworks	**D4-1 Cybersecurity Legal Frameworks**	**Dynamic**	• **R4-1:** Enhance international cooperation and mutual legal assistance in combating online criminal offences. • **R4-2:** Continue to push for stronger cybersecurity frameworks at the EU level and internationally.
	D4–2Legal investigation	**Strategic**	• **R4-3:** Strengthen national investigation capacity for computer-related crimes, with increased cooperation between the National Crime Agency and local police forces. • **R4-4:** Expand and allocate funding on work in training law enforcement in understanding computer related crime in order to support investigations, especially at local level. • **R4-5:** Enhance training and education of prosecutors and judges on computer related crimes. • **R4-6:** Allocate additional resources to cybersecurity education & training for prosecutors and judges. • **R4-7:** Introduce regular mandatory cybersecurity training for prosecutors and judges. • **R4-8:** Enhance investigative capacity and skills locally.
	D4-3 Responsible Reporting	**Formative**	• **R4-9:** Develop a responsible disclosure policy within public sector and facilitate its adoption in the private sector through targeted outreach, particularly in the CNI. • **R4-10:** Encourage cybersecurity behaviour rather than imposing CNIs to adhere to certain frameworks on vulnerability disclosure.

Dimension 5 Standards, organisations, and technologies	**D5-1 Adherence to standards**	**Established**	• **R5-1:** Establish a programme to strengthen government's capacity to adapt or adopt international standards to all scales of industry. • **R5-2:** Promote the adoption of international standards within the public sector. • **R5-3:** Promote awareness and implementation of standards among SMEs. • **R5-4:** Incorporate cybersecurity considerations in all stages of software and system development and processes. • **R5-5:** Adopt core development activities including configuration and document management, security development and lifecycle planning of software. • **R5-6:** Establish a process to measure the impact of standard adoption. • **R5-7:** Conduct risk assessment exercises in order to inform adherence to select standards. • **R5-8:** Embed security-by-design, in testing software.
	D5–2National Infrastructure Resilience	**Established**	• **R5-9:** Enhance the level of security processes in place (threat assessments and risk management processes). • **R5-10:** Document national resilience. • **R5-11:** Establish high-level security processes across private and government sectors especially for security risk management, threat assessment, incident response and business continuity. • **R5-12:** Conduct regular assessments of processes and national information infrastructure security according to standards and guidelines. • **R5-13:** Conduct assessments of national resilience for CNI and essential services to protect information systems of the country and the operators of CNI and essential services. • **R5-14:** Develop metrics to assess benefits for businesses from additional investments in technology. • **R5-15:** Invest in ICT research and cooperation between academia, research and industry to strengthen the software-engineering competencies of domestic ICT companies. • **R5-16:** Update security features in software architecture. • **R5-17:** Develop automated security functions in software and computer system configuration.
	D5-3 Cybersecurity Marketplace	**Established**	• **R5-18:** Promote sharing of information and best practices among organisations, to enhance covering of cybercrime insurance. • **R5-19:** Select coverage of cybercrime insurance based on strategic planning needs and identified risk. • **R5-20:** Consider the deployment of a government-backed cyber-reinsurance market.

Global Cyber Security Capacity Centre
Oxford Martin School, University of Oxford
Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,
United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk
Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home