

United Kingdom Country Report



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>



Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Dan Cimpean and Johan Meire.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

UNITED KINGDOM.....	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	7
NIS GOVERNANCE	13
OVERVIEW OF THE KEY STAKEHOLDERS.....	13
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS.....	15
FOSTERING A PROACTIVE NIS COMMUNITY	23
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	25
SECURITY INCIDENT MANAGEMENT	25
EMERGING NIS RISKS	26
RESILIENCE ASPECTS	28
PRIVACY AND TRUST.....	30
NIS AWARENESS AT THE COUNTRY LEVEL	31
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY.....	33
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	36
RELEVANT STATISTICS FOR THE COUNTRY	38
INTERNET ACCESS OF POPULATION AND ENTERPRISES	38
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS.....	39
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	40
THE UK CYBER SECURITY JOBS SURVEY.....	40
OTHER STATISTICS.....	42
APPENDIX.....	44
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	44
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	46
WARPs (WARNING, ADVICE AND REPORTING POINTS)	47
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	48
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY.....	49
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY.....	50
REFERENCES	51

United Kingdom

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader on the following Network and Information Security (NIS) related topics:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
 - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
 - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
 - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

2010 UK National Security Strategy (NSS) – key NIS highlights

On the 18th of October, 2010, the UK Government published¹ its new UK National Security Strategy (NSS) document called 'A Strong Britain in an Age of Uncertainty'. The NSS decides the priorities for action, and identifies 15 priority security risks to the UK. The following **Tier One** risks are judged by the National Security Council to be the highest priorities for UK national security:

- International terrorism, including through the use of chemical, biological, radiological or nuclear (CBRN) materials; and of terrorism related to Northern Ireland
- **Cyber attack**, including by other states, and by organised crime and terrorists
- International military crises and
- Major accidents or natural hazards.

This places the hostile attacks upon UK cyberspace by other states and large scale cyber crime at the same level as international terrorism, and international military threats². Additionally, potential severe disruption to information received, transmitted or collected by satellites, possibly as the result of a deliberate attack by another state are highlighted as **Tier Two** risks in the NSS.

The NSS document also highlights that UK business and government will need to work much more closely together to strengthen the defence against cyber attacks, so that if it happens, the country would be able to recover rapidly.

Cyberspace was evident in previous UK NSS documents but now has new emphasis. For example, the 2008 NSS document already suggested that any state-led threat to the UK was likely to be via cyber-attack or covert, technical attacks by foreign intelligence organisations rather than conventional military means.

2010 UK Strategic Defence and Security Review (SDSR) – key highlights³

The UK Strategic Defence and Security Review reflects the above-mentioned NSS priorities with a new transformative £650m CyberSecurity Programme over the next four years to protect the UK from cyber attacks from both nation states and individuals⁴.

The CyberSecurity Programme is aiming at closing the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyber space, and intends to:

- Overhaul UK approach to tackling cyber crime by creating a single point of contact where the public and businesses can report cyber crime;

¹ See the published 2010 UK National Security Strategy document 'A Strong Britain in an Age of Uncertainty' at www.direct.gov.uk

² As articulated in Com (2010) 673 final, Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 23 November 2010.

³ See the published 2010 UK Strategic Defence and Security Review document at www.direct.gov.uk

⁴ Cm 7048, Securing Britain in an age of uncertainty: The Strategic Defence and Security Review, HM Government, October 2010, Foreword

- Address deficiencies in the UK's ability to detect and defend itself against cyber attack – whether from terrorists, states, or other hostile actors. This will include:
 - ✓ improving UK's ability to deliver cyber products and services; and
 - ✓ enhancing UK's investment in national intelligence capabilities, focussing on the UK's centre for cyber security operations, working in cooperation with other government departments and agencies;
- Create a new organisation, the UK Defence Cyber Operations Group, to mainstream cyber security throughout the Ministry Of Defence (MOD) and ensure the coherent integration of cyber activities across the spectrum of defence operations. This will give MOD a more focussed approach to cyber, by ensuring the resilience of UK vital networks and by placing cyber at the heart of defence operations, doctrine and training. UK will also work to develop, test and validate the use of cyber capabilities as a potentially more effective and affordable way of achieving its own national security objectives;
- Address shortcomings in the critical cyber infrastructure upon which the UK as a whole depends. A new Cyber Team within the Department for Business, Innovation and Skills will provide strategic leadership and regulatory oversight for this;
- Sponsor long-term cyber security research, by working closely with research councils, the private sector and others;
- Introduce a new programme of cyber security education and skills. This programme will focus on awareness-raising to help encourage safe and secure online behaviour among the UK public;
- Continue to build cyber security alliances, including through the already strong relationship with the US and the establishment of new relationships with like-minded nations; and
- Establish a programme management office within the Office of Cyber Security and Information Assurance (in the Cabinet Office) to oversee, prioritize and coordinate the centralised funding and implementation of the Programme.

Further detail on how the UK CyberSecurity Programme will be implemented, for example, the ways in which the UK Government intends to work with the private sector, are likely be set out in further detail in the National Cyber Crime Strategy and the Cyber Security Strategy (both expected in 2011).

The regulatory framework

Data Protection/Privacy Legislation

In the United Kingdom, the EU Data Protection Directive (95/46/EC) has been implemented by the Data Protection Act (the "DPA" or the "Act"). The majority of its provisions came into force on 1st of March 2000.

The UK national regulatory authority responsible is the Information Commissioner's Office (the "ICO") that enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations.

The UK DPA gives rules for the way organisations must treat personal data and information, which apply to paper as well as electronic records. These rules are mandatory for all organisations that hold or process personal data, in the public as well as private and voluntary sector. The UK DPA contains eight data protection principles, stating that all data must be:

- Processed fairly and lawfully;
- Obtained & used only for specified and lawful purposes;
- Adequate, relevant and not excessive;
- Accurate, and where necessary, kept up to date;
- Kept for no longer than necessary;
- Processed in accordance with the individuals rights;
- Kept secure;
- Transferred only to countries that offer adequate protection.

eSignatures Legislation

The key eSignature legislative acts in place in the UK are still the Electronic Communications Act of 2000 and Electronic Signatures Regulations of 2002. No further significant developments incurred in 2010 linked to them.

- The Electronic Communications Act aims to help build confidence in electronic communications by creating a legal framework for electronic commerce and the use of electronic signatures, both in the private and public sectors.
- The Electronic Signatures Regulations complete this act and implements in the UK law the European Directive 1999/93/EC on a Community framework for electronic signatures.

eIdentification/eAuthentication⁵

The UK Government introduced the Identity Documents Bill to Parliament on 26 May 2010. The Bill makes provision for the cancellation of the UK National Identity Card, the Identification Card for EEA nationals and the destruction of the National Identity Register.

UK attempted to implement a national e-ID card for its citizens as well as for non-nationals planning to reside in the UK for more than three months. However, recent governmental changes brought the cancellation of this e-ID scheme⁶.

⁵ Source: *Study on eID Interoperability for PEGS: Update of Country Profiles* - <http://ec.europa.eu/idabc/servlets/Docb482.pdf?id=32522>

⁶ Source: http://www.ips.gov.uk/cps/rde/xchq/ips_live/hs.xsl/1972.htm

UK also has a series of soft signature certificates, issued by accredited CSPs, for both natural and legal persons. The national identifier used in this country is the National Identity Registration Number. Some sector specific identifiers also exist:

- The National Insurance number, issued for all persons eligible for employment in the UK. This number is unprotected, and used also for social security and tax administrations.
- The National Health Service (NHS) number, issued for all persons eligible for health care in the UK. This number is unprotected and presently not linked to a central database.

The identity register used for natural persons in the UK is the National Identity Register. However, identity data is not systematically collected in a single database in this country. As for legal entities (limited liability entities established in the UK), they are registered in the Companies House database.

An authentic source principle has been informally adopted through horizontal integration of identity sources. Also, authentication policies have been formally adopted by the UK government. The UK government's Strategic Action Plan distinguishes a number of authentication means based on damage risks through the "Registration and Authentication – e-Government Strategy Framework Policy and Guidelines Version 3.0", but does not implement a strict hierarchy between these.

PKI identification systems are in place, for the British Chamber of Commerce and Equifax, based on soft qualified signature certificates. Non-PKI systems are also implemented, notably for the Government gateway which is based on a single factor login (username/password). Also worth noting is the fact that UK is a partner in the STORK⁷ (Secure idenTity acrOss borders linKed) project that aims to establish an European eID interoperability platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID.

The consortium members include national authorities, non profit organisations, private companies and academic partners from: Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom and Iceland.

Cybercrime legislation

Computer Misuse Act

In the United Kingdom, the key legislative instrument regarding attacks against computer systems and data is the Computer Misuse Act of 1990 which outlaws the unauthorised modification of data stored or transmitted by IT systems, as well as unauthorised access to such systems.

It remains the primary piece of UK legislation focusing on the misuse of computer systems. It covers crimes such as hacking and the deliberate spread of viruses, and was created to prevent unauthorised access to or modification of computer systems and to deter criminal elements from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. It is important to note that computer crime cases are heard in exactly the same way as regular criminal trials.

There is a range of other legislation in the UK dealing with offences utilising computer systems and networks, for example using computers or the Internet to facilitate fraud is covered by offences in fraud legislation.

⁷ The STORK project consortium consists of 29 participants representing 13 Member States and Iceland. A full list of participants in the STORK project is available at www.eidstork.eu

A recent, well covered by media⁸, case of enforcement of the UK cybercrime legislation consisted of the arrest in January 2011 by the Metropolitan Police Central e-Crime Unit (PCeU) of five men in connection with offences under the Computer Misuse Act 1990. The men were arrested in relation to the denial of service attacks on firms that withdrew support for Wikileaks after its controversial release of classified US diplomatic cables. The PCeU said the arrests relate to recent distributed denial of service (DDoS) attacks against several companies by an online group calling themselves 'Anonymous'.

Computer Crimes covered by the Police and Justice Act 2006 Chapter 48 that amends the Computer Misuse Act (Part 5 sections 35-38)

Several articles of the UK are of relevance in the NIS context, as they directly address the computer misuse and the unlawful access to, or use of, information. The new amendments came into force on October 1, 2008, and reads as follows:

35 Unauthorised access to computer material	<p>(1) In the Computer Misuse Act 1990 (c. 18) ("the 1990 Act"), section 1 (offence of unauthorised access to computer material) is amended as follows.</p> <p>(2) In subsection (1)-</p> <p style="padding-left: 20px;">(a) in paragraph (a), after "any computer" there is inserted ", or to enable any such access to be secured";</p> <p style="padding-left: 20px;">(b) in paragraph (b), after "secure" there is inserted ", or to enable to be secured,".</p> <p>(3) For subsection (3) there is substituted - "(3) A person guilty of an offence under this section shall be liable-</p> <p style="padding-left: 20px;">(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;</p> <p style="padding-left: 20px;">(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;</p> <p style="padding-left: 20px;">(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."</p>
36 Unauthorised acts with intent to impair operation of computer, etc	<p>For section 3 of the 1990 Act (unauthorised modification of computer material) there is substituted- "3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.</p> <p>(1) A person is guilty of an offence if-</p> <p style="padding-left: 20px;">(a) he does any unauthorised act in relation to a computer;</p> <p style="padding-left: 20px;">(b) at the time when he does the act he knows that it is unauthorised;</p> <p style="padding-left: 20px;">(c) either subsection (2) or subsection (3) below applies.</p> <p>(2) This subsection applies if the person intends by doing the act-</p> <p style="padding-left: 20px;">(a) to impair the operation of any computer;</p> <p style="padding-left: 20px;">(b) to prevent or hinder access to any program or data held in any computer;</p> <p style="padding-left: 20px;">(c) to impair the operation of any such program or the reliability of any such data; or</p> <p style="padding-left: 20px;">(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.</p> <p>(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.</p> <p>(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-</p> <p style="padding-left: 20px;">(a) any particular computer;</p> <p style="padding-left: 20px;">(b) any particular program or data; or</p> <p style="padding-left: 20px;">(c) a program or data of any particular kind.</p> <p>(5) In this section-</p> <p style="padding-left: 20px;">(a) a reference to doing an act includes a reference to causing an act to be done;</p> <p style="padding-left: 20px;">(b) "act" includes a series of acts;</p> <p style="padding-left: 20px;">(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.</p>

⁸ See the article published on: http://www.computerweekly.com/Articles/2011/01/27/245111/Police-arrest-five-men-over-Wikileaks-related-39Anonymous39-denial-of-service.htm#Scene_1

- (6) A person guilty of an offence under this section shall be liable-
- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
 - (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;
 - (c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both."

37 Making, supplying or obtaining articles for use in computer misuse offences

- After section 3 of the 1990 Act there is inserted-
- "3A Making, supplying or obtaining articles for use in offence under section 1 or 3
- (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
- (2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
- (3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.
- (4) In this section "article" includes any program or data held in electronic form.
- (5) A person guilty of an offence under this section shall be liable-
- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
 - (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;
 - (c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

Computer Misuse Act 1990 Chapter 18

- 1. Unauthorized access to computer material:**
- (1) A person is guilty of an offence if-
- (a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer, or to enable any such access to be secured,
 - (b) the access he intends to secure, or to enable to be secured, is unauthorized, and
 - (c) he knows at the time when he causes the computer to perform the function that that is the case.
- (2) The intent a person has to have to commit an offence under this section need not to be directed at:
- (a) any particular program or data,
 - (b) a program or data of any particular kind, or
 - (c) a program or data held in any particular computer.
- (3) A person guilty of an offence under this section shall be liable-
- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
 - (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;
 - (c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.
- 2. Unauthorized access with intent to commit or facilitate commission for further offences.**
- (1) A person is guilty of an offence under this section if he commits an offence under section 1 above (" the unauthorized access offense") with intent
- (a) to commit an offense to which this section applies; or
 - (b) to facilitate the commission of such an offense (whether by himself or by any other person); and the offense he intends to commit or facilitate is referred to below in this section as the further offense.
- (2) This section applies to offences
- (a) for which the sentence is fixed by law; or
 - (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by

section 33 of the Magistrates Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offense is to be committed on the same occasion as the unauthorized access offense or on any future occasion.

(4) A person may be guilty of an offense under this section even though the facts are such that the commission of the further offense is impossible.

(5) A person guilty of an offense under this section shall be liable

(a) on summary conviction, to imprisonment for a term not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if-

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act-

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section-

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

Enforcement is mainly carried out by the Serious and Organised Crime Agency (SOCA) and by the Metropolitan Police Central e-Crime Unit (PCeU).

UK Government Security Policy Framework (HMG Security Policy Framework)

The UK Security Policy Framework (SPF) represents a new and innovative approach to protective security and risk management in the UK Government, grouped around seven security policies:

- Security Policy No. 1: Governance, Risk Management and Compliance
- Security Policy No. 2: Protective Marking and Asset Control
- Security Policy No. 3: Personnel Security
- Security Policy No. 4: Information Security and Assurance
- Security Policy No. 5: Physical Security
- Security Policy No. 6: Counter-Terrorism
- Security Policy No. 7: Business Continuity

In general terms, the framework is aimed primarily at UK Government's departments and agencies in supporting their protective security and counter-terrorism responsibilities - however, it does have wider application. The commercial sector plays an increasingly intimate role within the UK Government matrix, as well as making up the core sectors within the Critical National Infrastructure.

The 'Data Handling Procedures in Government' was published by the Cabinet Office in June 2008, and have now been formalised into a new Information Assurance Standard (i.e. IA Standard no.6); 'Handling Personal Data and Managing Information Risk. It is important to stress here that these are the minimum requirements; it is expected that many departments and agencies will manage their specific security risks over and above these baseline measures, using sound risk management principles as outlined within the framework⁹.

Particular role in developing these had the Centre for Protection of National Infrastructure (CPNI), based within the Security Service and the National Technical Authority for Information Assurance (CESG) based within the Government Communication Headquarters, who have provided expertise and support to the Cabinet Office's Government Security Secretariat.

⁹ See: <http://www.cabinetoffice.gov.uk/spf>

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	<ul style="list-style-type: none"> • Office of Cyber Security and Information Assurance (OCSIA) • Centre for the Protection of the National Infrastructure (CPNI) • Department for Business, Innovation and Skills (BIS) • Communications-Electronics Security Group (CESG) • Ofcom • Information Commissioner's Office (ICO) • Cyber Security Operations Centre (CSOC) • Serious Organized Crime Agency (SOCA) • Police Central e-crime Unit (PCeU)
CERTs	<ul style="list-style-type: none"> • BP DSAC - BP Digital Security Alert Centre • BTCERTCC • CITIGROUP (UK) • CSIRTUK • DAN-CERT - DANTE Computer Emergency Reponse Team • DCSIRT - Diageo CSIRT • ECERT - Energis Squared Limited CERT • ESISS • EUCS-IRT • GovCertUK - CESGs Government Computer Emergency Response Team • JANET CSIRT • MLCIRT (UK) • MODCERT – Ministry of Defence Computer Emergency Response Team • OxCERT - Oxford University IT Security Team • Q-CIRT - QinetiQ Computer Incident Response Team • RBSG-ISIRT - Royal Bank of Scotland Group Information Security Incident Response Team • RM CSIRT (Royal Mail CSIRT CC)
WARPs	<ul style="list-style-type: none"> • NEGWARP • NWWARP • YHWARP • EMGWARP • WMCWARP • CY2WARP • EEWARP • LCWARP • SEGWARP • SWWARP • Scotland WARP • Northern Ireland WARP • CY1WARP • MODWARP • NHSWARP • PoIWARP • NUWARP • LS1WARP • TGRWARP • RAYWARP • GUWARP
Industry Organisations	<ul style="list-style-type: none"> • Electronic Communications Resilience and Response Group (EC-RRG) • OWASP - The OpenWeb Application Security Project

	<ul style="list-style-type: none"> • British Computer Society - Information Security Specialist Group (BCS-ISSG) • Information Security Awareness Forum • tScheme • The UK Technology Industry (Intellect) • British Security Industry Association (BSIA) • Mobile Industry Crime Action Forum (MICAF)
Academic Organisations	<ul style="list-style-type: none"> • Institute for Information Security Professionals (IISP) • Royal Holloway University of London
Others	<ul style="list-style-type: none"> • Cyber Security Challenge UK • ISACA (Information Systems Audit and Control Association) – UK Chapter • British Standards Institute (BSI) • ISCA • BCS Security Forum • Information Assurance Advisory Council (IAAC)

For contact details of the above-indicated stakeholders we refer to the ENISA “Who is Who”¹⁰ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory¹¹.

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

¹⁰ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

¹¹ <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation and information exchange via OCSIA

The Office of Cyber Security & Information Assurance (OCSIA) supports the UK Security Minister, and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK.

The OCSIA alongside the Cyber Security Operations Centre work with lead government departments and agencies such as the Home Office, Ministry of Defence (MoD), Government Communications Headquarters (GCHQ), CESG, the Centre for the Protection of National Infrastructure (CPNI) and the Department for Business, Innovation and Skills (BIS) in driving forward the cyber security programme for UK government and give the UK the balance of advantage in cyberspace.

Co-operation and information exchange via BIS

This Department for Business Innovation and Skills (BIS) - Cyber Team focuses on activities, both domestic and international, aimed to embed good security practice within the UK.

Since the early 1990s until 2008 BIS (in partnership with industry) produced a biennial Information Security Breaches Survey, intended to help businesses understand the information security risks they face¹². In partnership with Mid Yorkshire Chamber of Commerce & Industry (MYCCI), BIS helped produce an interactive e-learning package which reinforces the importance of information security awareness – see also the awareness section of this report.

BIS represents the information security needs of businesses, both within the UK and internationally, to promote the development of appropriate international standards and a regulatory framework that is conducive to the uptake of electronic commerce. In particular BIS is a member of the Management Board of the European Network and Information Security Agency (ENISA).

In September 2010, the Department for Business Innovation and Skills (BIS) has launched a consultation process asking for suggestions and proposals for implementing the revised EU Electronic Communications Framework, which UK must implement by May 2011. According to the revised EU Electronic Communications Framework, in some instances the obligations on Member States, national regulatory authorities and industry are extended, particularly with regard to: consumer protection; e-privacy; and security and resilience of networks and services.

A specific consultation document was communicated by BIS: "Implementing the revised EU Electronic Communications Framework – Overall approach and consultation on specific issues" - setting out the UK preferred approach to implementation and asks questions on a limited number of specific issues. There is the potential that some of these new obligations could create an additional regulatory burden for business – this was assessed as far as possible in a separate impact assessment document.

¹² The 2008 Survey (the main Technical Report and the Executive Summary) is available to download or order from www.security-survey.gov.uk

Co-operation and information exchange via CPNI

CPNI considers that sharing of information about the risks facing networks is beneficial to both government and industry, and that this allows a stakeholder to learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities to competitors or to media.

CNI partners are working with CPNI in Information Exchanges – these mechanisms are based upon the personal trust of representatives, sharing information in a confidential meeting, run under a version of the Chatham House Rule. Trust is built up slowly; representatives at Information Exchanges are expected to attend all meetings, which are held every two months. Each organisation can put forward a maximum of two representatives, and cannot send substitutes to attend; in order to not inhibit the sharing of sensitive information.

ADMIE	The Aerospace and Defence Manufacturer's Information Exchange was formed in December 2006, to share confidentially mutually beneficial information regarding electronic security threats in the aerospace and defence sector. The ADMIE comprises UK-based organisations involved in this sector. Contact point for enquiries: admie@cpni.gsi.gov.uk
CIPSIE	The Communications Industry Personnel Security Information Exchange was formed in April 2010 out of the Telecommunications Industry Security Advisory Council 'people' workstream, to share confidentially mutually beneficial information regarding personnel security threats, vulnerabilities and incidents between its members. The CIPSIE comprises UK-based organisations involved in this sector. Contact point for enquiries: cipsie@cpni.gsi.gov.uk
FSIE	The UK Financial Services Information Exchange was formed in February 2003, to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the UK financial sector. The FSIE includes members from UK-based financial organisations including banking, insurance, securities, service providers, exchanges and CPNI. Contact point for enquiries: fsie@cpni.gsi.gov.uk
MSPIE	The Managed Service Providers Information Exchange consists of commercial organisations that supply IT services and security to UK CNI customers in the public and private sector. The main aim is to understand risks better and improve security to the benefit of customers, clients, stakeholder and UK national security through information sharing and cooperation. The MSPIE achieves this by facilitating the sharing of information in a confidential and trusted environment concerning threats, vulnerabilities and incidents of electronic attack between its membership. Contact point for enquiries: mSPIE@cpni.gsi.gov.uk
NIXIE	The Northern Ireland Cross-Sector Information Exchange (NIXIE) was formed in October 2008 to enable infrastructure companies based in, or operating in, Northern Ireland to share in confidence mutually beneficial information between its members regarding physical, personnel and information security threats, vulnerabilities, incidents and solutions. The NIXIE includes members from the communications, energy, finance and water sectors and CPNI.
NSIE	The UK Network Security Information Exchange (UK-NSIE) was formed in April 2003 to share sensitive information in the information and communications technologies sector. It currently includes IP providers; core mobile operators; and traditional telecommunications providers, as well as CPNI. Participating companies now cover over 80% of the telecommunications market in the UK. It is linked to NSIE in USA, of which BT is a member. BT acts as the channel for information between the two Exchanges. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include: a

guide to the procurement of resilient telecoms; best practice guidance on the secure implementation of BGP.

Contact point for enquiries: nsie@cpni.gsi.gov.uk

PIIE The **Pharmaceutical Industries Information Exchange** was formed in September 2006 to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the pharmaceutical industry. All of the PIIE members are from global pharmaceutical corporations that have a significant UK interest.

Contact point for enquiries: piie@cpni.gsi.gov.uk

SCSIE The **SCADA and Control Systems Information Exchange** is for those companies that are dependent upon SCADA (Supervisory Control and Data Acquisition) or other process control or telemetry systems. Formed in October 2003, it shares confidential and mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the SCADA and process control environment. The SCSIE includes members from UK-based energy, transport and water companies. It has produced and is currently working on good practice guidance. Completed guidance includes: Implement secure architecture, understanding business risk, firewall deployment for SCADA and process control networks to name but a few.

Contact point for enquiries: scsie@cpni.gsi.gov.uk

E-SCSIE The **European SCADA and Control Systems Information Exchange** aims for European industry, government and research to benefit from the ability to collaborate on a range of common issues, and to focus effort and share resource where appropriate. The outcome is a raised level of protection adopted across Europe's SCADA and Control Systems.

Contact point for enquiries: scsie@cpni.gsi.gov.uk

TSIE The **Transport Sector Information Exchange** was formed in September 2006 and expanded coverage of the aviation sector Information Exchange to include other major transport methods.

Contact point for enquiries: tsie@cpni.gsi.gov.uk

VSIE The **Vendor Security Information Exchange** was formed in January 2005 to share confidentially mutually beneficial information regarding electronic security threats among the major companies involved in the ICT industry. The VSIE comprises members of major international companies in the ICT sector.

Contact point for enquiries: vsie@cpni.gsi.gov.uk

SRIE The **Security Researchers Information Exchange** was formed in November 2006 to share confidentially mutually beneficial information regarding electronic security threats in the penetration testing and security research sector. The SRIE comprises of members of UK penetration testing and security research companies.

Contact point for enquiries: srie@cpni.gsi.gov.uk

In addition to the Information Exchanges already facilitated by CPNI, other exchanges will be set up, both in the UK and internationally.

CPNI is creating channels through which information in one Information Exchange is passed to others; a channel exists between the UK and US Network Security Information Exchanges. Another communication channel exists between CPNI and the corresponding Canadian authorities.

Co-operation via WARPs

The UK WARP programme¹³ is part of the Information Sharing Strategy of the UK Centre for the Protection of National Infrastructure (CPNI). WARPs (short for Warning, Advice, and Reporting Points) are one way an organisation can share information with the centre from which the lessons can be abstracted and shared.

The WARPs have been developed to provide a cost effective method to support defence against attacks. Their purpose is to provide a specific community with the capability to share security related information - both problems and solutions - and thereby to develop more secure and responsive environments. The UK WARP directory¹⁴ lists all WARPs which are currently operational or due to go live in the future.

UK WARP operators fora are organised in both a virtual and a physical form. Virtual, via an electronic discussion forum and physical as a face to face meeting held four times per year. Meetings have been hosted by Local and Central Government, Academia and the Private Sector and have been held in venues across the country from London to the East and West Midlands, Merseyside and Yorkshire.

WARP Operators, WARP Member Representatives, GovCertUK (the Computer Emergency Response Team for UK Government) and Representatives from other Government Departments make up the regular attendees. Occasional invites are offered to representatives from Industry and other interested parties as required.

Co-operation and information exchange via EC-RRG, on resilience aspects

The Electronic Communications Resilience and Response Group (EC-RRG, previously TI-EPF), was established to ensure the availability of electronic communications infrastructure for the UK and to provide an industry emergency response capability through the ownership and maintenance of the National Emergency Plan for Telecommunications¹⁵.

EC-RRG's members include:

- Network operators that provide key aspects of the national telecommunications infrastructure (including but not limited to Category 2 responders as defined by the UK Civil Contingencies Act of 2004);
- LINX, representing the Internet sector;
- Telehouse Europe, representing the data warehouse sector;
- Airwave Solutions Ltd, that provides the secure and resilient mobile telecommunications system for the Emergency Services;
- Ofcom, the UK telecommunications regulator;
- BIS, Department for Business Innovation and Skills that has lead responsibility for telecommunications within government;
- UK Cabinet Office, Civil Contingencies Secretariat;
- CPNI, Centre for the Protection of National Infrastructure;
- UK Ministry of Defence;
- Government Office SE, the office with lead responsibility for telecommunications and
- Representatives from the Scottish Executive and Welsh Assembly.

¹³ See: www.warp.gov.uk

¹⁴ See the UK WARP directory at: www.warp.gov.uk/directory.html

¹⁵ See the UK National Emergency Plan for Telecommunications document, available at: <http://interim.cabinetoffice.gov.uk/media/418987/nep-telecomms-sector-march2010.pdf>

In view of the importance of communications in responding to emergencies Telecommunications sub-groups are to be established, as appropriate, within the existing resilience infrastructures. Each sub-group will be responsible for considering all aspects of communications, including the technical means, and how resilience might be enhanced within their area.

EC-RRG has an arrangement in place, referred to as NEAT (the National Emergency Alert for Telecommunications), which supports co-operation across the industry in response to emergencies affecting telecommunications in the UK.

NEAT is a protocol for sharing information among members of the EC-RRG, and is triggered in the event of circumstances that may effect the operation of telecommunications networks. The process provides a conduit for information between industry members of EC-RRG, between industry and government and within members' organisations that enables the widest possible picture of impacts to be assessed. Members of EC-RRG meet virtually and assemble a situation report. The report provides a shared understanding of the situation which becomes central to determining actions that are needed to rectify any identified problems.

NEAT has been central to providing a telecommunications sector response to incidents that have included: the bombs in Central London (2005); the explosion and fire that engulfed the oil depot at Buncefield, England (2005) and the flooding that inundated Gloucester in central England (2007).

The NEAT protocol was integrated into Exercise White Noise a Department for Business Innovation and Skills (BIS) led exercise held in November 2009 that simulated a sector response to a major telecommunications incident. Exercise White Noise formed part of the National Preparedness Programme annual exercise series and brought together the relevant parts of Government, including the Devolved Administrations, with industry partners to test the response to a failure of the UK telecommunication network. The end of exercise report ¹⁶ provides an overview of the exercise and key learning points.

Confidence in the NEAT protocol is maintained through regular testing that contact can be established with members and specific aspects of the protocol have been exercised annually since 2004 through the EMPEX exercise programme.

Co-operation and information exchange via CESG

An informative newsletter¹⁷ is issued by the Communications-Electronics Security Group (CESG) to improve communications between CESG, UK Government and industry.

In September 2010, CESG organised the IA10 event that brought together representatives from the UK Government, industry and academia. The event was centred on the following key topics:

- **Shared Services Risk Management:** Government cannot afford to waste resources duplicating the building or assurance of systems. Neither can it afford to miss the business opportunities that sharing information brings. This stream focused on management of risks in the delivery and use of shared services and shared information as efficiently as possible;
- **Building Secure Systems:** this stream focused on how good architectural design coupled with good enterprise security management can deliver world class information assurance at low cost;

¹⁶ See the available post exercise public report of the Exercise White Noise available at: <http://interim.cabinetoffice.gov.uk/media/427527/bis-exercise-white-noise.pdf>

¹⁷ See the CESG AGENDA Autumn 2010 - IA10 Conference Special Edition available at: http://www.cesg.gov.uk/publications/media/cesg_agenda_ia10_a_perfect_storm.pdf

- **Cyber-Network Defence:** drawing on senior industry as well as government speakers, this stream focused on providing a greater understanding of the real threats facing government networks – and what can be done to protect them;
- **People, Culture and Professionalisation:** while IA09 recognised the importance of culture and people in managing information risk. IA10 further developed these ideas while considering the impact of the current climate.

Co-operation and information exchange via CERTs

UKCERTs is an informal forum ¹⁸of UK CSIRT teams with participants from the government, academic, corporate and commercial CERTs. The forum has quarterly meetings of up to 25 members, with presentations provided by team members and invited information security experts. The forum is designed to encourage co-operation and information sharing between the participants. UK WARP teams also recently attended the meetings, enhancing the relationship between the UK CSIRT and WARP communities.

JANET (UK) is holding an annual JANET CSIRT Conference. The event includes presentations from the community and cover a range of topics within computer and network security, as for example: Incident Response & Legal Developments, Boundaries of Responsibilities, Information Security 2.0.

GovCertUK, part of the Communications-Electronics Security Group (CESG) manages and coordinates the response activity to electronic attack incidents that have an impact on the Government community within the UK. GovCertUK also works closely with the Centre for the Protection of National Infrastructure (CPNI), who coordinates the response activity to electronic attacks against the UK Critical National Infrastructure (CNI).

Electronic attack incidents that impact on UK systems may also be affecting similar organisations internationally, therefore GovCertUK works closely with other national CERTs from around the world, to identify emerging attacks, share information and to resolve issues outside our national boundaries.

MODCERT is responsible for coordinating the UK's Ministry of Defence response to computer security incidents. MODCERT is a member organisation of both the international Federation of Incident Response Security Teams (FIRST) and the Trusted Introducer (TI) scheme, which aim to provide a mechanism for computer security incident information to be shared amongst communities of interest.

MODCERT is a distributed organisation, consisting of a central Co-ordination Centre (the Joint Security Co-ordination Centre or JSyCC), and a number of Monitoring and Reporting Centres (MRCs), Warning, Advice and Reporting Points (WARPs), and Incident Response Teams (IRTs). MODCERT works closely with CSIRTUK and the GovCertUK at the national Infrastructure Security Co-ordination Centre, also known as UNIRAS.

¹⁸ See: www.ukcert.org.uk/

Co-operation and information exchange via Ofcom

With respect to the NIS domain, in 2010 Ofcom issued a discussion document¹⁹ for its stakeholders seeking views on the key issues on net neutrality and traffic management. Ofcom intention was to help stimulate debate on this topic and to collect insight from the key stakeholders via a series of roundtables with industry, citizen and consumer groups interested to participate in these discussions. This discussion was planned to take place in two phases: Phase 1 – Summer/Autumn 2010 and the Phase 2 – Autumn 2010 - Spring 2011.

Interaction via the Serious Organised Crime Agency (SOCA)

SOCA was formed in 2006 when the National Hi-Tech Crime Unit (NHTCU) was merged with the National Criminal Intelligence Service (NCIS), the National Crime Squad, and parts of Her Majesty's Revenue and Customs (HMRC) and the Immigration Service. The agency has responsibility for fighting cybercrime and online fraud, among other areas of organised crime.

A Confidentiality Charter was developed in the past by the NHTCU²⁰ to help business to interact with it in a secure, efficient and confidential manner when wishing to exchange information, and especially when reporting hi-tech crime, or seek advice. However, after the Serious Organised Crime Agency²¹ (SOCA) has replaced the NHTCU, there is no longer a Confidentiality Charter, which allowed firms to report computer attacks directly to the NHTCU with a guarantee of privacy. The charter was established in the past because many firms were reluctant to report security breaches to the police, for fear of damage if the details became public.

According to the consultation paper²² launched in July 2010 by the UK Home Secretary, it appears that several changes will incur on change how the UK Government handles serious crime, including computer-related offences. In the view of this consultation paper, a new UK National Crime Agency will lead the fight against organised crime and the protection of UK borders. It will harness and exploit the intelligence, analytical and enforcement capabilities of the existing Serious Organised Crime Agency (SOCA), but better connect these capabilities to those within the police service, HM Revenue and Customs, the UK Border Agency and a range of other criminal justice partners.

Interaction via the UK e-Crime Congress

Entering its 9th year, the March 2011 e-Crime Congress is providing practical insights on how best to proactively reduce electronic risk, delivering critical information on emerging threats to IT systems and data assets, and detailing examples of best practice that can be adopted to defend against technically sophisticated and complex cyber attacks.

The e-Crime Congress plans to bring together senior decision makers and technical experts from 45 countries and an overall international audience of over 500 professionals from global business, government departments, and law enforcement agencies.

Those invited from international law enforcement agencies in 2011 include representatives from: Australia, Belarus, Belgium, Brazil, Bulgaria, Canada, Finland, France, Georgia, Germany, Ghana, Hong Kong, Hungary, India, Indonesia, Israel, Italy, Japan, Kenya, Korea, Latvia, Lithuania, Mauritius, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Panama, Philippines, Poland,

¹⁹ See the "Traffic Management and 'net neutrality'" document published by Ofcom at:

<http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf>

²⁰ The ex-National Hi-Tech Crime Unit (NHTCU), currently replaced by SOCA

²¹ See: <http://www.soca.gov.uk/>

²² See: <http://www.homeoffice.gov.uk/publications/consultations/policing-21st-century/table-one?view=Html>

Romania, Russia, Serbia, Spain, Sweden, Switzerland, Trinidad & Tobago, UAE, Ukraine, USA and Vietnam.

Being a platform for sharing strategic, operational, and tactical knowledge the 2011 e-Crime Congress focuses on the following key themes²³:

- **Analysing the latest e-Crime trends** to effectively prioritize mitigation strategy and defend against sophisticated attack profiles;
- **Evolving e-security and risk management frameworks** in response to shifts in the technological and business environment;
- **Adapting to changes in the threat landscape** to ensure the protection of key targets, eliminate weak points, and mitigate high-impact risks;
- **Improving response and investigations capabilities** to quickly identify incidents or events and close gaps in the attack surface;
- **Protecting online, client facing revenue channels** from compromise to prevent losses and improve business processes

Public Private Partnership

In the Fifth Report published by the European Union Committee of the UK House of Lords - "Protecting Europe against large-scale cyber-attacks", there are several relevant conclusions with respect to the public private partnership in the NIS area, in UK. For illustration²⁴:

- In their written evidence towards the European Union Committee of the UK House of Lords the UK Government indicates that the United Kingdom had adopted a public private partnership model, where Government maintained a close working relationship with industry on a voluntary basis to ensure communications resilience—including that of the Internet. Their view was that to date this model had proved successful in enhancing the resilience of the communications sector.
- In the view of the European Union Committee of the UK House of Lords, despite good intentions, the involvement of Internet entrepreneurs in the formulation of UK Government policy is as yet at best superficial. Both the Government and the Commission seem to think that it is for the private sector to come forward. The European Union Committee of the UK House of Lords thinks that, on the contrary, it is for the public sector to take the initiative and to offer to experienced Internet entrepreneurs a real say in how public private partnerships are best developed.

²³ See: <http://www.e-crimecongress.org/congress/website.asp?page=home>

²⁴ See the full version of the published by the House of Lords, European Union Committee - Fifth Report Protecting Europe against large-scale cyber-attacks, at: <http://www.publications.parliament.uk/pa/ld200910/ldselect/ldcom/68/6802.htm> . Ordered to be printed 9 March 2010 and published 18 March 2010.

Fostering a proactive NIS community

International co-operation via the European Government CERTs (EGC) group

CSIRTUK and GovCertUK are amongst the active members²⁵ of the European Government CERTs (EGC) group. EGC is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.

To achieve this goal, the EGC group members:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Encourage formation of government CSIRTs in European countries
- Communicate common views with other initiatives and organizations.

International co-operation via the Commonwealth Telecommunications Organisation (CTO) Cyber Security Forum

With the critical information infrastructure of Estonia coming under attack in 2007, the focus of cyber security was elevated from an individual perspective to a national perspective. Importantly this incident highlighted the need for developing countries to implement robust and effective cyber security frameworks.

With “Common Responses to a Global Challenge” as its main theme, the Commonwealth Telecommunications Organisation (CTO) was convening a Cyber Security Forum on 17-18 June 2010, hosted by the Department for Business, Innovation and Skills (BIS).

The aims of this annual forum²⁶ were to:

- Create awareness of the many types of cyber threats and alert stakeholders in Commonwealth countries to the need to adopt robust cyber security frameworks;
- Build the capacity of the key decision makers in developing countries to implement strategies aimed at preventing and responding to the growing menace of cyber crime;
- Provide the key decision makers with the means to adopt resilient technical measures, establish appropriate organisational structures and create robust legal and regulatory frameworks;
- Promote international cooperation in cyber security to help developing countries to leverage the strengths of developed countries;
- Broker partnerships between the different players in cyber security to facilitate the flow of information, expertise and resources.

The keynote speakers were the UK Minister of Security and the Deputy Secretary General of the Commonwealth Secretariat. The main sessions will include contributions from ministers and experts from across the Commonwealth, the UK’s Office of Cyber Security and the Department for

²⁵ The members of the European Government CERTs group include: Austria - GovCERT.AT, Finland - CERT-FI, France - CERTA, Germany - CERT-Bund, Hungary - CERT-Hungary, Netherlands - GOVCERT.NL, Norway - NorCERT, Spain - CCN-CERT, Sweden - CERT-SE, Swiss - GovCERT.ch, United Kingdom - CSIRTUK, United Kingdom - GovCertUK; See more details at: <http://www.egc-group.org/>

²⁶ See: <http://www.bis.gov.uk/assets/biscore/business-sectors/docs/cyber-security-2010-agenda.pdf>

Business, Innovation and Skills (BIS). There were also speakers from the Internet Corporation for Assigned Names and Numbers (ICANN), the UK Children's Coalition on Internet Safety, the Serious Organised Crime Agency (SOCA) and the European Economic and Social Committee (EESC).

Interaction via the 2011 London Worldwide Cybersecurity Summit organised by the EastWest Institute and co-hosted by London First

The second Worldwide Cybersecurity Summit will be organised in London, UK on 1-2 June 2011 and will continue the work of the first summit (in 2010 in Dallas, US) bringing together leaders of governments, businesses and civil society from around the world to determine new measures to ensure the security of the world's digital infrastructure.

The Worldwide Cybersecurity Summit in London is organised by the international, non-partisan, not-for-profit policy organisation EastWest Institute, and is co-hosted by London First. The programme plans²⁷ to cover the following NIS-relevant topics:

- Improved international standards and agreements for supply chain integrity;
- A harmonized global framework for fighting cyber crime, with case studies from the financial services sector;
- A 24/7 emergency response system tying together all countries and territories connected to the internet;
- International arrangements for priority communications in crisis or emergency;
- Multilateral agreements on cyber conflict and rules of engagement;
- Transparency and international information sharing on cyber attacks;
- Protection of youth;
- Private sector leadership in problem solving for sector interests;
- Best-in-class research and analysis from China, Russia and India on building trust and other political aspects of cybersecurity policy;
- New examples of cross-border youth engagement in personal protection and privacy issues.

²⁷ See: <http://www.cybersummit2011.com/programme>

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

Reporting electronic attack incidents via CPNI

CPNI co-ordinates intelligence and develops advice on information systems vulnerabilities and electronic attack threats. In support of this function, CPNI has to gather data concerning electronic attack incidents in order to evaluate the ever-changing threat. The threat can be most easily assessed from the various types of attack that the community is observing in real time, and the primary source of such information is therefore from the community itself. As such, a variety of electronic attack (eA) incidents can be reported to CPNI:

- Network probes and scans;
- Blocked hacking attacks where there are clear indications that a network or system has been attacked;
- Malware blocked due to suspicious process activity detected by heuristic anti-virus scanning (not malware routinely blocked by anti-virus software);
- Actual malicious software infection;
- Successful hacking attacks;
- Malicious denial of service attacks;
- Data interception and monitoring;
- Other anomalous behaviour, malware, hacking or exploitation of new vulnerabilities (zero-day) in hardware or software systems.

CPNI is not a law enforcement agency and incidents relating to criminal activity is be reported via the UK police service portal²⁸.

Organisations that are part of CSIRTUK (CPNI Combined Security Incident Response Team) community are encouraged to report information security incidents to the CSIRTUK. By working with other agencies as required, CSIRTUK provides advice and assistance in managing the response to the event, and advises on how to manage the response to incidents and produces advisories on security matters.

CSIRTUK collects information on about potential security vulnerabilities, incidents or events, whether in the electronic, physical or personnel security spheres from national infrastructure organisations. This information is treated as confidential, and if necessary, particulars that would identify individuals or organisations are removed so the information can be incorporated into generic security advice. In this way, valuable experience can be shared to help other UK stakeholders. By enhancing the traditional CERT role to cover holistic advice - covering physical, personnel and electronic issues - CSIRTUK provides a central point for reporting security incidents and for receiving advice and guidance.

²⁸ See: www.police.uk

Emerging NIS risks

The UK national risk assessment process

In UK, the national risk assessment process takes place at different levels:

- Risk assessment at the UK government level
- Risk assessment at the regional and local level
- Risk assessment in the devolved administrations

The risk assessment process is performed in line with published guidance²⁹. At all these levels there is a certain focus on the risks related to communication networks and information security.

Risk assessment at the UK government level

The UK Government monitors the most significant emergencies that the country and its citizens could face over the next five years through the classified UK National Risk Assessment (NRA)³⁰. This confidential assessment is conducted annually, since 2005, and draws on expertise from a wide range of departments and agencies of government.

The UK National Risk Register (NRR)³¹ is the public outcome of the NRA version and this 2010 edition has been produced to reflect the latest iteration of the National Risk Assessment.

The NRA and NRR are intended to capture the range of emergencies that might have a major impact on all, or significant parts of, the UK. These are events which could result in significant harm to human welfare: casualties, damage to property, essential services and disruption to everyday life. The NRA, and therefore the NRR, only look at risks of emergencies in the UK, not throughout the world. The risks cover three broad categories:

- Natural events,
- Major accidents and
- Malicious attacks.

The UK National Risk Register – key updates on the NIS topics

The UK Government committed to publishing a National Risk Register (NRR) in its first National Security Strategy, and has undertaken to update it regularly. The first National Risk Register was published in August 2008, and was based on the secret National Risk Assessment for that year.

The updated version of the UK National Risk Register is based on the 2009 iteration of the National Risk Assessment. For this, consultation has been done through workshops with cross-Government stakeholders, businesses and community groups, and by means of a survey of Regional and Local Resilience Forums. The overseeing Steering Group included experts from central and regional UK Government, emergency responders, community representatives and business groups.

The main changes brought by the 2010 edition of the National Risk Register, with respect to the Network and Information Security (NIS) areas consist of the fact the NRR risk matrix does now

²⁹ See: <http://interim.cabinetoffice.gov.uk/ukresilience/preparedness/risk.aspx>

³⁰ *Idem*

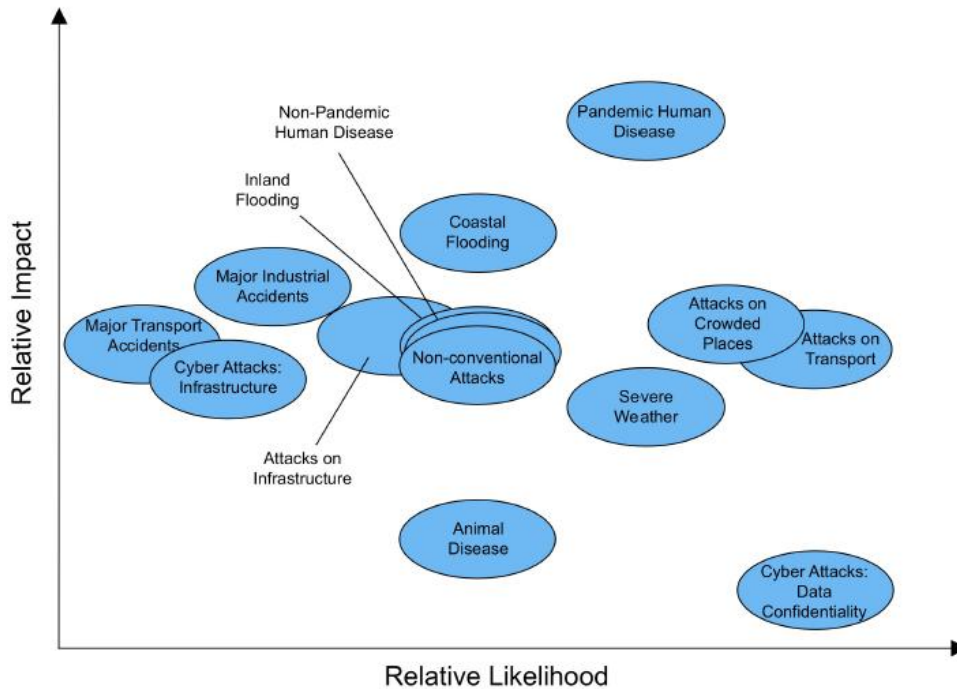
³¹ See: http://interim.cabinetoffice.gov.uk/intelligence-security-resilience/civil-contingencies-uk-resilience/national_risk_register.aspx

provide greater detail on NIS risks and also reflects changes in the underpinning UK National Risk Assessment matrix³²:

- 'Electronic Attack' has been renamed 'Cyber Attack' to move the NRR closer to the UK Cyber Security Strategy³³ ;
- The matrix now contains two cyber attack risk groupings to give greater granularity to the threat:
 - a. 'Cyber Attacks: National Infrastructure' and
 - b. 'Cyber Attacks: Data Confidentiality'.

Figure 1 - UK NRR

National Risk Register of Civil Emergencies: 2010 Edition
 An illustration of the high consequence risks facing the United Kingdom



The risk and impact of cyber attacks on IT and communication systems varies greatly according to the particular sectors affected and the source of the threat. Cyber attacks have the potential to export, modify or delete information or cause systems to fail.

There is a known risk to commercially valuable and confidential information in some government and private sector systems from a range of well resourced and sophisticated attacks. Cyber attack may be used more widely by different groups or individuals with various motives.

³² See: <http://www.cabinetoffice.gov.uk/resource-library/national-risk-register>

³³ See the June 2009 version of the UK Cyber Security Strategy at: http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

Risk assessment at the regional and local level

In UK, alongside the national level risk assessments, regional and local tiers are required to produce a specific risk assessment that reflects, as far as possible, the unique characteristics of each region and local area.

The UK Government provides and publishes guidance³⁴ to Local Resilience Forums (LRFs) and Regional Resilience Forums (RRFS)s on the likelihoods of emergencies based on national assessments, which can then be flexibly tailored to meet local and regional judgements of the risks facing their areas. This ensures there is a fully integrated risk assessment process at all levels of Government which underpins coherent emergency planning throughout the UK.

Community Risk Registers (CRR) capture how risks relate to a certain local area in UK. The CRRs are approved and published by Local Resilience Forums which include representatives from local emergency responders as well as public, private and voluntary organisations.

The UK Community Risk Registers – key updates on the NIS topics

Community Risk Registers (CRR)³⁵ have been developed across the UK by emergency services and other responders as a means of assessing the risks that a particular area may contend with and the impact that these will have on that area. By area:

The majority of these CRRs already include NIS-specific risks. Two examples of NIS-specific risks that are assessed³⁶ in the UK CRRs are:

- No notice loss of significant telecommunications infrastructure in a localised fire, flood or gas incident;
- Telecommunication infrastructure – human error.

Resilience aspects

Enhancing the resilience of everyday telecommunications in UK

The UK Government's strategy for enhancing resilience is formalised and published on the web site of the Cabinet Office. Guiding principles for enhancing the resilience of communications were published on the web site of the Cabinet Office, including advice see towards achieving resilient telecommunications and a survey of some available technical solutions.

An important step in enhancing resilience is to help ensure that responders avail themselves of the best possible value from commercial telecommunication services. In UK, steps have already been taken to raise awareness through newsletters, workshops and interim guidance.

The UK Centre for the Protection of National Infrastructure (CPNI) has produced guidance³⁷ on enhancing the resilience of telecommunications networks and services.

³⁴ See the published *Local Risk Assessment Guidance (LRAG)*

http://interim.cabinetoffice.gov.uk/media/131921/ep_ann_04b.pdf

³⁵ See the list of UK CRRs at the following link:

http://www.direct.gov.uk/en/HomeAndCommunity/InYourHome/Dealingwithemergencies/Preparingforemergen-cies/DG_176587

³⁶ See, for exemplification, the published CRR of Cumbria:

<http://www.cumbriaresilience.info/home.asp?ID=CRR&MenuID=22>

³⁷ See the telecommunications resilience guidance produced by CPNI, available at:

www.cpni.gov.uk/Docs/Telecommunications-resilience-v3.pdf

Relevant resilience courses at the Emergency Planning College³⁸ have also been reviewed and extensively revised to support Telecommunications Sub-Groups that have been established to take forward the agenda of enhancing the resilience of telecommunications in each Local Resilience Forum (LRF) area.

The UK Electronic Communications Resilience and Response Group (EC-RRG, previously TI-EPPF), is established to ensure the availability of Electronic Communications infrastructure for the UK and provide an industry emergency response capability through the ownership and maintenance of the National Emergency Plan for Telecommunications³⁹.

EC-RRG has an arrangement in place, referred to as NEAT (the National Emergency Alert for Telecommunications), which supports co-operation across the industry in response to emergencies affecting telecommunications in the UK. Membership of the Group embraces Category 2 Telecommunications Responders (as defined by the Civil Contingencies Act of 2004). In view of the importance of communications in responding to emergencies Telecommunications sub-groups are to be established, as appropriate, within the existing resilience infrastructures. Each sub-group will be responsible for considering all aspects of communications, including the technical means, and how resilience might be enhanced within their area.

UK communication systems used in responding to an emergency situation

The communication systems used in responding to an emergency have been updated in line with the Civil Contingencies Act 2004 to mirror how organisations structure themselves in responding to local, regional and national emergencies.

The systems and procedures employed to safeguard the UK communication networks at periods of high loading, which typically occur during major incidents are identified in a Joint Doctrine Publication 02 (JDP 02), 2nd Edition dated September 2007 promulgated as directed by the UK MOD Chiefs of Staff⁴⁰.

³⁸ See the web page of the Cabinet Office Emergency Planning College: www.epcollege.com

³⁹ See the UK National Emergency Plan for Telecommunications document, available at: <http://interim.cabinetoffice.gov.uk/media/418987/nep-telecomms-sector-march2010.pdf>

⁴⁰ See: <http://www.cabinetoffice.gov.uk/sites/default/files/resources/defencecontribution1.pdf>

Privacy and trust

Personal Data and Sensitive Personal Data

The UK Data Protection Act 1998 defines personal data to mean any data relating to living individuals who can be identified from: (i) the data; or (ii) the data and other information which is, or is likely to come into, the possession of the data controller, including expressions of opinion and indications of the data controller in respect of that individual. This definition is therefore closely based on the standard definition of personal data.

The requirement that personal data "relate to" an individual was considered by the Court of Appeal, which suggested that there are two notions which may be used to help decide whether information could be considered to be "personal data". The first is whether the information is "biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised". The second is that the information should have the data subject as its focus rather than some other person or event such as an investigation into some other body's conduct.

Under the UK DPA, sensitive personal data includes both: (i) the standard types of sensitive personal data; and (ii) information about criminal offences or criminal proceedings.

Sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. A range of additional processing conditions are set out both in the DPA and in a separate Order including processing for equal opportunities monitoring, regulatory investigations, research and political activities.

Information Security aspects in the local implementation of the Data Protection Directive

The DPA addresses general data security obligations but does not contain specific security requirements. However, ICO issued guidance⁴¹ recommending, amongst others, the use of encryption – especially on mobile devices – or adoption of ISO 27001.

Data protection breaches and enforcement aspects

The DPA does not contain any obligation to inform the Information Commissioner (ICO) or data subjects of a security breach. However, the Information Commissioner has issued guidance stating he expects to be informed of any serious security breaches. Moreover, data controllers in certain sectors may be required to inform sectorial regulators of any breach (for example, financial services firms may be required to inform the Financial Services Authority of any breach).

Concerning the enforcement of the UK DPA, it is noted that ICO has the power to issue an Enforcement Notice for breaches of data protection, and it can impose substantial fines (e.g. up to 500.000 £) on the organisations that deliberately or recklessly commit serious breaches of the UK DPA. Appeals from such notices are heard by the Information Tribunal, an independent body set up specifically to hear cases concerning enforcement notices or decision notices issued by the ICO.

A new legislation approved in 2009 gives the ICO the power to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act.

⁴¹ See: http://www.ico.gov.uk/tools_and_resources.aspx

NIS awareness at the country level

Awareness actions targeting the consumers/citizens

Data Protection

In a move to mark European Data Protection Day, the UK Information Commissioner's Office (ICO), supported by the Ministry of Justice, is urging people to take more care on social networking sites, before giving out their personal details online, and to understand what to do when things go wrong.

UK ICO monitors awareness and understanding of the UK Data Protection Act and Freedom of Information Act on an annual basis, and completes an annual track report⁴² for both individuals and organisations.

To help online users understand how to surf safely, the ICO has re-launched its Personal Information Toolkit⁴³ that includes tips on how to protect personal details online as well as setting out people's rights to access and correct the information that is held about them. The previous version of the toolkit has been requested by over 100,000 members of the public, to date.

Get Safe Online

Launched in 2005, Get Safe Online was established to provide a source of unbiased, user-friendly advice about online safety to UK consumers and micro-businesses. Since its inception, it has operated as a joint initiative between UK Government, the Serious Organised Crime Agency (SOCA), and private and public sponsors from the worlds of retail, technology, finance and communications. Compared with 2009, no Get Safe Online Report was published in UK for 2010.

One relevant development is that in 2010 the UK National Fraud Authority (NFA) did become a sponsor of Get Safe Online, the UK's national internet security awareness initiative. The announcement was made at the inaugural meeting of the UK e-Crime Reduction Partnership.

Other major supporters of Get Safe Online in UK include the Cabinet Office, Home Office, BIS, SOCA, Ofcom, ISSA UK chapter, NGOs and several business organisations. The NFA's role in the initiative forms part of its broader efforts to unite the UK's counter-fraud community and implement the Government's National Fraud Strategy.

Awareness actions targeting the UK Government bodies

Awareness actions via the Communications-Electronics Security Group (CESG)

The Communications-Electronics Security Group (CESG), being the information assurance arm of the GCHQ (UK Government Communications Headquarters), develops the UK policy for protecting data and advises on its implementation.

CESG takes a balanced view of risk to identify appropriate countermeasures, thereby giving a sound basis from which to make informed decisions on managing the risks to data.

This work is managed by the CESG's information assurance policy unit as a 'common-good' activity on behalf of all UK government departments and agencies. The guidance CESG produces is intended mainly for this audience, but may also have relevance for local government and others in the public sector.

⁴² See: http://www.ico.gov.uk/about_us/research/corporate.aspx

⁴³ See: www.ico.gov.uk

Areas where CESG issues policy and guidance include:

- Securing electronic government services to the citizen
- Securing government connections to the Internet
- Securing the connection of business domains
- Assessing security needs for systems and networks
- Protection against hacking and computer viruses
- Approving the security of government IT systems
- Disposing of computer media used for sensitive information
- Passwords and other methods of authentication
- Interpreting and implementing national information assurance policy and standards.

High-level information assurance policy originated by CESG is issued to government users under Cabinet Office auspices, either as part of the Security Policy Framework⁴⁴ or in the Information Security Standards series. Manuals supplement these in greater detail.

There is also a wide range of private-sector organizations that work with the public sector to promote information assurance awareness. These include:

- The Information Assurance Advisory Council;
- The British Computer Society,
- The Internet Security Forum,
- The National Computing Centre,
- The Internet Watch Foundation,
- The Confederation of British Industry,
- The Institute of Information Security Professionals,
- European Information Society Group,
- Royal United Services Institute,
- Chatham House.

Awareness actions via BIS

In partnership with Mid Yorkshire Chamber of Commerce & Industry (MYCCI), BIS helped produce the interactive e-learning package named Bob's Business™ - an eLearning tool ⁴⁵which reinforces the importance of information security awareness, in order to reduce the risk and frequency of security incidents within UK companies.

⁴⁴ To obtain copies of CESG policies, the reader shall contact the CESG Enquiries, CESG, Room A2j, Hubble Road, Cheltenham, Gloucestershire GL51 0EX, UK or telephone 01242 709141.

⁴⁵ See: www.bobs-business.co.uk

Country-specific activities for identifying and promoting economically efficient approaches to information security

BIS assessed the potential that some of the new obligations triggered by the revised EU Electronic Communications Framework could create an additional regulatory burden for UK business. This was assessed in a BIS impact assessment which was published as well in September 2010⁴⁶. The EU Electronic Communications Framework is based on the following directives:

- the "Access" Directive (2002/19/EC) ;
- the "Authorisation" Directive (2002/20/EC)
- the "Framework" Directive (2002/21/EC)
- the "Universal Service" Directive (2002/22/EC)
- the "E-Privacy" Directive (2002/58/EC)

Although the aim of many of the amendments to the EU Electronic Communications Framework is to improve the overall regulatory framework for business and where possible to reduce regulatory burdens in the case of spectrum markets, in some instances the regulatory powers of Member States, national regulators, and the Commission itself are being extended, particularly with regard to consumer protection, e-privacy, and security and resilience.

In some instances this brings the Framework in line with current UK practice, thus helping to limit the additional regulatory burden on the UK. In the Impact Assessment made ⁴⁷by BIS, a brief summary of the main proposals is set out (see the table below) along with a qualitative assessment of the high level impacts of their implementation:

Directive	Summary of Policy	Benefits/Costs
Framework Directive	The Framework Directive seeks to establish a harmonised framework for regulation of electronic communications networks and services, associated facilities and services, and following these changes, the regulation of certain aspects of terminal equipment to facilitate access for disabled users and hence the promotion of equality and diversity. It also lays down the tasks of national regulators and establishes procedures to ensure harmonised application of the regulatory framework across all Member States.	+ Enhanced opportunities for infrastructure sharing to enable duct access thus facilitating greater investment in superfast broadband. + Benefits from ensuring resilience of networks and services. - Costs to business of new security and resilience provisions. - Costs to Ofcom from monitoring security and resilience. - Article 12(4) allows national authorities to request information from undertakings in order to provide a detailed picture of the infrastructure in a Member State. There will be a cost to request this information. - Cost to business from providing the 'competent national authority' with the above information. + Removal of regulatory burdens that hinder the introduction of spectrum leasing. + Potential for efficiencies from possible review of appeals regime governing NRA.
Access Directive	The Access Directive further harmonises the way in which Member States regulate access to and interconnection of electronic communications networks and associated facilities. The aim is to establish a regulatory framework in accordance with internal market principles to promote competition, interoperability and consumer benefits. A	+ Potential increase in competition from express powers to NRA to enforce functional separation on undertakings with SMP. (This is a discretionary power – The NRA will be able to enforce functional separation should they believe there to be benefits from doing so) + Benefits for business of greater legal certainty regarding the powers and

⁴⁶ See the BIS impact assessment published at: www.bis.gov.uk/Consultations/revised-eu-electronic-communications-framework

⁴⁷ Idem

Directive	Summary of Policy	Benefits/Costs
	<p>fundamental principle here is the provision of access to incumbent networks – breaking into monopolies – and the rules on which that is based. It also covers how the regulator might intervene to bring it about with explicit reference to the availability of functional separation as a market remedy.</p>	<p>responsibilities of NRAs. + Potential for greater investment if NRAs are required to take account of investment in regulatory decisions. - Possible costs given greater regulatory powers of NRAs.</p>
Authorisation Directive	<p>The Authorisation Directive looks to simplify the rules and conditions governing the authorisation required to provide electronic communications networks and services in order to better facilitate the provision of these services throughout the European Community. In so doing it further facilitates the internal market providing for harmonisation of what Member States are allowed to do and not allowed to do with an overall goal of levelling the playing field. The intention is to prevent Member States from introducing rules which prevent other operators from starting up or doing business.</p>	<p>+ Improvements in management of spectrum through effective and efficient use and associated benefits to business. - Costs to Ofcom from review of spectrum licenses granted for 10 years or more that can not be transferred or leased. + Greater innovation through reduced barriers of entry to spectrum - Costs to Ofcom to review general authorisation and licenses within two years of the Directive coming into force. + Consumer benefits from Ofcom being able to take action after a breach has been remedied. - Costs to business of providing evidence of compliance with the conditions of rights of use of radio frequencies to Ofcom, however this is a limited extension to current practice and is not very extensive.</p>
Universal Services Directive	<p>Provisions in the Universal Service Directive are intended to strengthen consumer protection by:</p> <ul style="list-style-type: none"> • Improving the transparency of information from service providers to consumers, including information on supply conditions and on tariffs. • Setting a time limit of one working day for 'porting' (transferring) a telephone number following a change of fixed or mobile operator. • Enhancing the implementation of '112' emergency services, including by ensuring greater access to caller location information. <p>In addition the Universal Service Directive also updates and strengthens provisions in the area of eAccessibility and the rights of users with disabilities. New provisions include:</p> <ul style="list-style-type: none"> • A requirement to ensure equivalent access by disabled users to 112 emergency services • A power for Ofcom to impose equivalence obligations on all operators, not just BT. • An obligation on Government to promote the availability of terminal equipment for disabled users. <p>Some of these new obligations set out current UK practice and so will not constitute a new regulatory burden as such. Others empower (but do not require) Ofcom to impose regulation, while others are expected to have some impact on the regulatory burden of operators. In all cases, however, the ultimate goal is to promote the interests of consumers, whether through facilitating competition or</p>	<p>+ Benefits to consumers from greater availability of information about supply conditions and tariffs. Much of this information is already provided to consumers in contracts in the UK. + Greater efficiency of emergency services operations due to enhanced access to caller location information. + Increased competitive intensity as a result of an increased level of switching due to a reduction in barriers to number porting. + Increased benefits to consumers as a result of being able to exploit welfare gains from switching. - Costs incurred by operators as a result of moving to faster number porting. + Benefits from increased opportunities and engagement in the digital economy for disabled users. - Potential cost to business to pay for any services mandated should Ofcom use their power to impose equivalence obligations on all operators.</p>

Directive	Summary of Policy	Benefits/Costs
E-Privacy Directive	<p>protecting vulnerable groups.</p> <p>This Directive sets out the fundamental rights and freedoms of EU citizens when using electronic communications. In particular, it strengthens rights to privacy and confidentiality with respect to the holding and processing of personal data by network and service providers.</p> <p>The key changes to this Directive are:</p> <ul style="list-style-type: none"> • The introduction of a duty on providers of electronic communications services to notify personal data breaches to the Information Commissioner’s Office; • A need for penalties, including criminal penalties where appropriate, for breaches of the Directive; • A change in the requirement for storing information on a subscriber’s or user’s equipment from a ‘right to refuse’ to obtaining consent. 	<p>+ Benefits of improved consumer welfare (through higher take-up of services which would also be mirrored by benefits to business) as a result of potential reduced incidences of breaches of personal data due to all three key changes proposed.</p> <p>+ Improvements to industry reputation as a result of fewer complaints.</p> <p>- Familiarisation costs associated with dealing with guidance.</p> <p>- Costs to Information Commissioner’s Office of producing guidance.</p> <p>- Costs to browser owners from having to provide users with information about cookies and how to change the browser settings.</p>

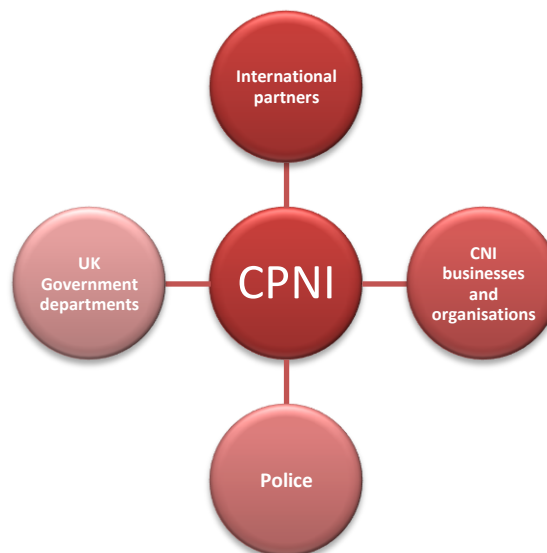
Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

Improving UK Critical Information Infrastructure Protection

The UK Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides protective, integrated security advice (combining information, personnel and physical) to the businesses and organisations which make up the national infrastructure.

CPNI works with a variety of partners to reduce the vulnerability of the national infrastructure, focusing in particular on UK Critical National Infrastructure (CNI). Key partners include government departments with responsibility for infrastructure sectors; businesses and organisations within those sectors that own or operate critical infrastructure; and other security specialists and advice delivery partners including the Police.

Figure 2 - Partners of CPNI



The formal definition of the UK's CNI is: "Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life". In this context it is relevant to mention that CPNI has issued, on behalf of the Government Cross-Sector Working Group (CSWG) for CNI, a framework and guidance document with the purpose to set the framework for government's programme of work to protect the nation's infrastructure.

The framework covers the definitions and criteria used to distinguish between 'critical' infrastructure and wider national infrastructure; the UK national approach to managing risks and prioritising effort; and the roles and responsibilities of different government bodies. It is intended to provide clarity and a common foundation for activity by all those in the UK government involved in national infrastructure protection. Although developed primarily for a government audience, it is shared with the key industry stakeholders on whom success of the infrastructure protection programme relies.

A system has been introduced for categorising infrastructure according to its value or 'criticality', determined on the basis of the impact of its loss. This categorisation is done using the UK Government 'Criticality Scale' which assigns categories for different degrees of severity of impact.

Category 5 ('CAT 5') indicates infrastructure the loss of which would have the most severe impact; CAT 0 indicates infrastructure whose loss would be minimal when considered in the national context.

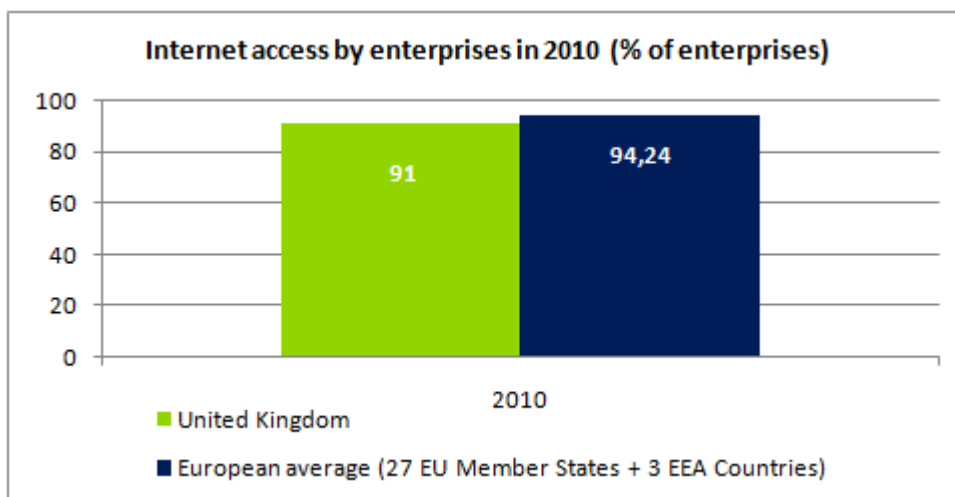
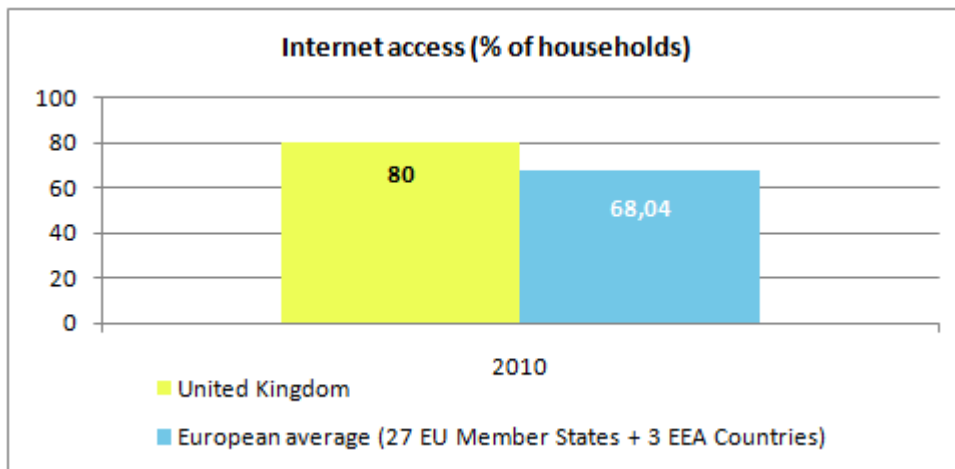
Data about the UK's Critical National Infrastructure (i.e. CATs 3-5) is stored in a central database held by CPNI. This data is shared with Police Counter Terrorism Security Advisers (CTSAs) and Chairs of Local Resilience Fora. The database also holds details of the wider national infrastructure (i.e. CATs 2 and below). Mapping tools are being developed which will enable geographic visualisation and interrogation of the data.

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in UK, a series of relevant statistics are included in this section. Some of them indicate that the information society in UK is at a relatively advanced stage of development in comparison with the European average, while others show interesting trends.

Internet access of population and enterprises

The following graphs provide an overview of the situation⁴⁸ of Internet access in UK for enterprises and respectively households, relative to the European average.

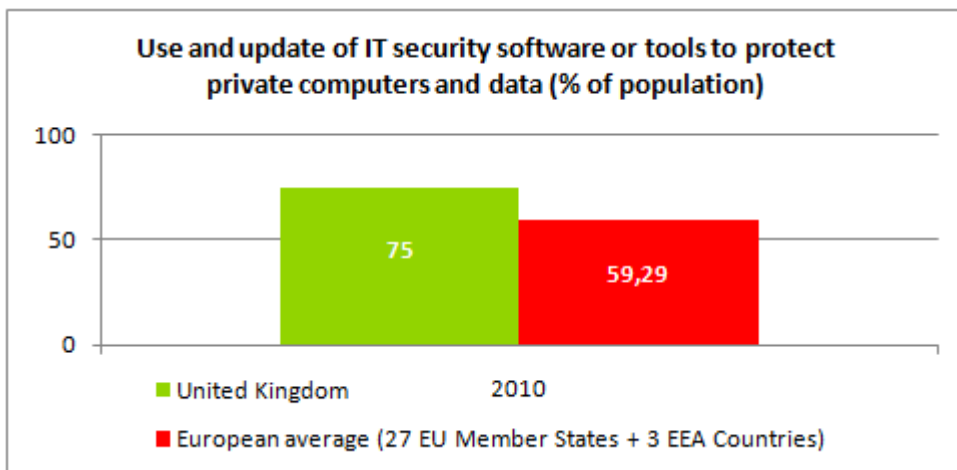
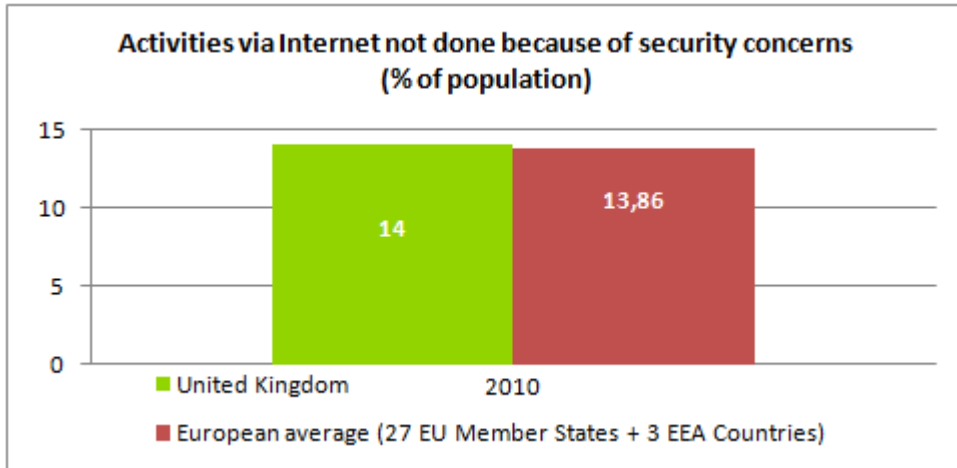


Based on 2010 data, the statistics indicate that the enterprises in UK have almost the same level of Internet access as the European average, while for the households, the UK internet access is above the European average.

⁴⁸ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

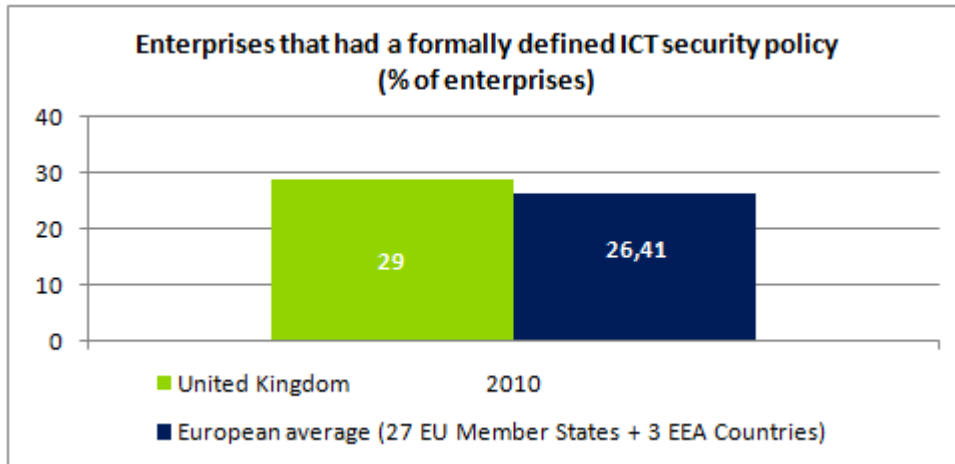
The percentage of population in UK that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is in line with the European average:



Meanwhile, it appears that the use of security software or tools to protect private computers and data is significantly above the European average, indicating a higher level of overall awareness on the need of using such security measures.

Statistics on use of Internet by enterprises and related security aspects

Enterprises in UK have a formally defined ICT security policy, at a percentage level that is comparable with their European peers.



The UK Cyber Security Jobs Survey

SANS Institute, a founder sponsor of Cyber Security Challenge UK, recently funded an industry survey⁴⁹ which demonstrates the requirement for the UK cyber security professionals.

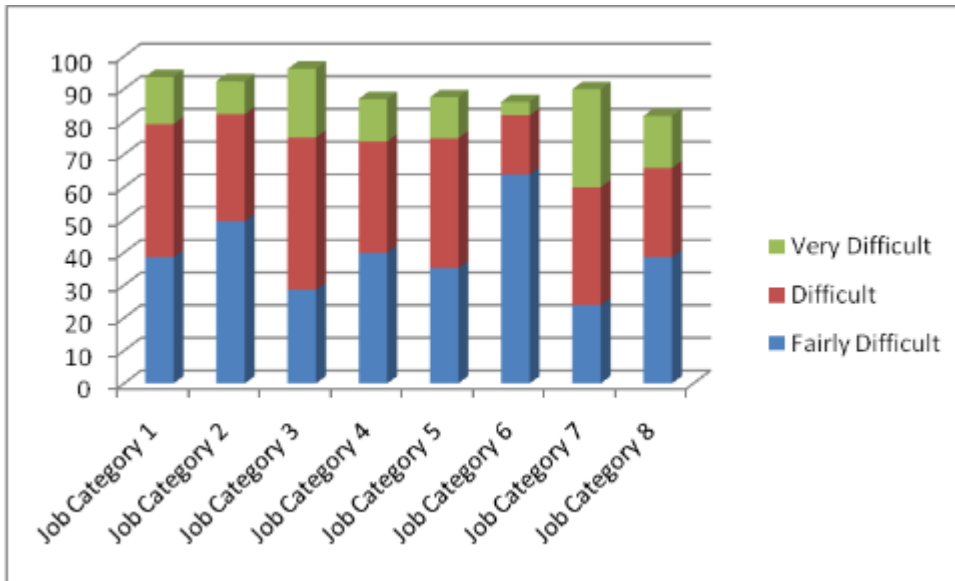
The survey does covers aspects related to the following cyber security job categories, as they were defined by the Institute of Information Security Professionals (IISP):

Cyber security job categories	Details
Job Category 1	Strategy, Policy, Governance. Strategist, Policy Manager, ITSO, DSO, CISO.
Job Category 2	Risk Management, Verification and Compliance. Risk Analyst, Risk Assessor, Business Information Security Officer, Reviewer, Auditor.
Job Category 3	Incident and Threat Management and Response. Incident Manager, Threat Manager, Forensics – computer – mobile and network – analyst, CSIRT, Attack Investigator, Malware analyst, Penetration Tester, Disaster Recovery, Business Continuity.
Job Category 4	Operations and Security Management. Network Security Officer, Systems Security Officer, Information Security Officer, Crypto custodians, Information Managers.
Job Category 5	Engineering, Architecture & Design. Architect, Designer, Development, Secure coding, software design and development, applications development. Security tools, Implementation.
Job Category 6	Education, Training and Awareness. Security Programme Manager.
Job Category 7	Research. Security Researcher.
Job Category 8	Lawyer for advice and prosecution regarding data protection and Internet crime.

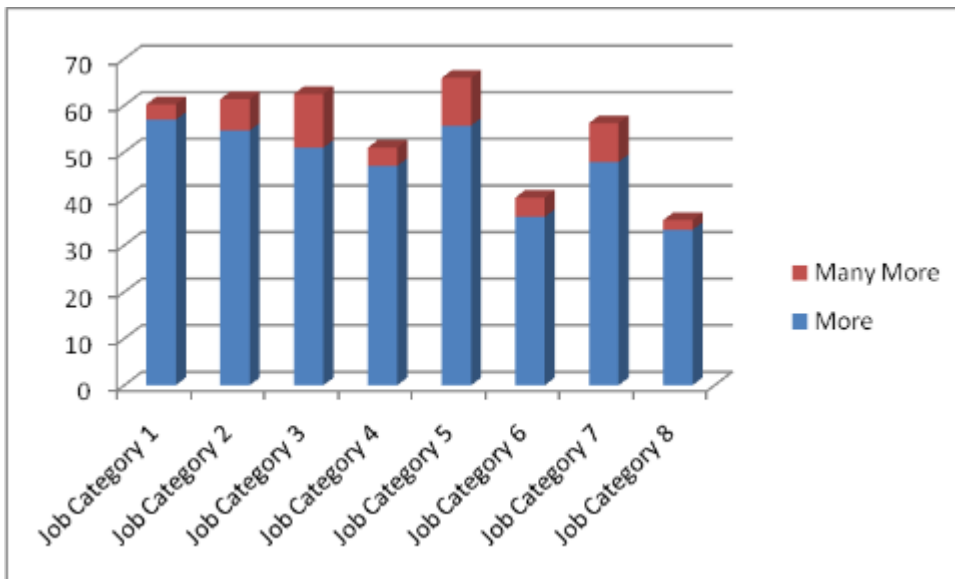
Over 90% of those surveyed indicated that it is difficult to recruit to cyber security jobs. The most problematic were those in incident response and threat assessment but policy, strategy and governance jobs came a close second. This graph⁵⁰ shows the percentage of respondents who found difficulty in recruiting to each of the 8 surveyed job categories:

⁴⁹ See: <https://cybersecuritychallenge.org.uk/about/cyber-security-jobs-survey.html>

⁵⁰ Source: Cyber Security Jobs Survey published and available on <https://cybersecuritychallenge.org.uk/>



Nearly 60% of the respondents thought that in UK would be a need for more jobs in cyber security in all 8 job categories. The biggest increase was predicted to be in jobs in architecture, engineering and design but incident and threat management came a close second. This graph shows the percentage of respondents who expected an increase in the number of jobs in the next 5 years by job categories.

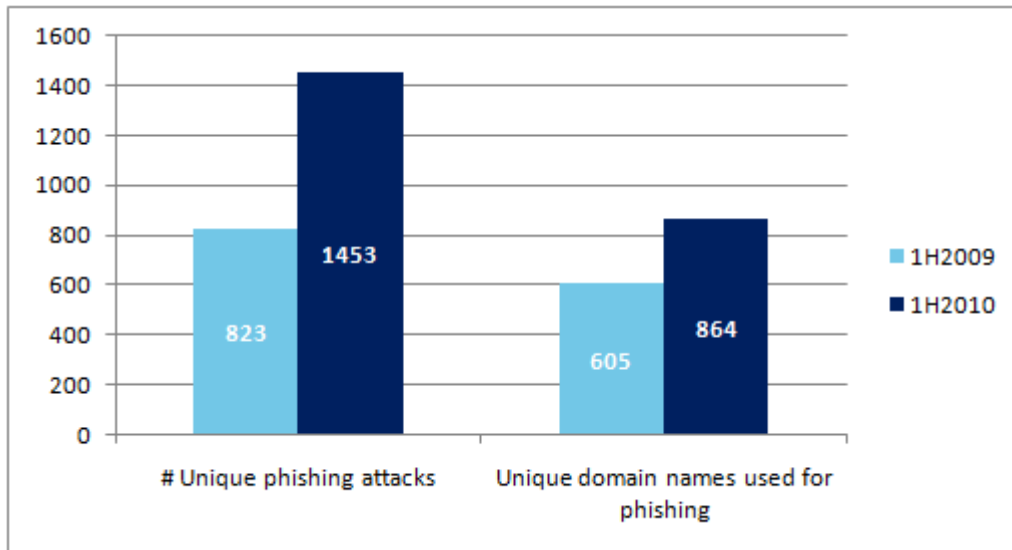


Other Statistics

The UK SDSR claims that criminal groups have already registered over 9,500 Olympic Games-related web addresses. It also states that 51% of all the malicious software threats that have ever been identified were identified in 2009 alone.

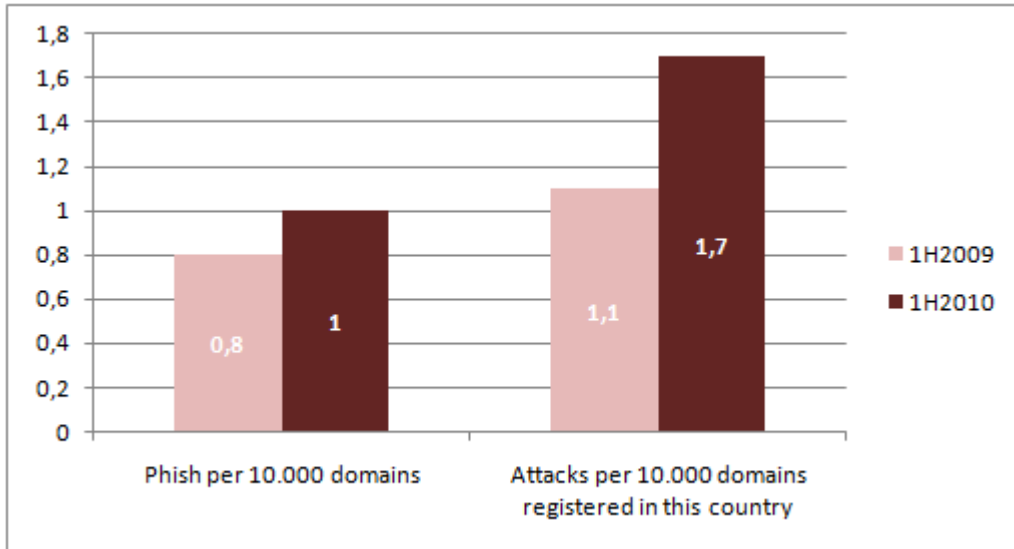
Recent UK press coverage has also reported⁵¹ on incidents such as the Stuxnet virus' ability to target software used in industrial processes. The virus allegedly attacked systems at Bushehr, Iran's first nuclear power plant, thus further highlighting the potential for cyber attacks to affect a country's critical infrastructure.

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, UK was mentioned in the global report⁵² published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



⁵¹ See also: Falliere, N. (2010). Exploring Stuxnet's PLC Infection Process. Available at (last accessed 23 January 2011): <http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process>

⁵² See: Global Phishing Survey: Trends and Domain Name Use 1H2010, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf



A survey⁵³ published by the Information Commissioner’s Office (ICO) in January 2011, has revealed that 80% of people are concerned about protecting their personal information online. Moreover, 96% of individuals surveyed are concerned that organisations do not keep their details secure, and a further 60% believe that they have lost control of the way their personal information is collected and processed.

⁵³ The ICO’s full research report is available at: http://www.ico.gov.uk/about_us/research/corporate.aspx

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Office of Cyber Security and Information Assurance (OCSIA)	<p>OCSIA supports the Security Minister and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK.</p> <p>Alongside the Cyber Security Operations Centre OCSIA works with lead government departments and agencies such as the Home Office, MoD, GCHQ, CESG, CPNI and BIS in driving forward the cyber security programme for UK government and give the UK the balance of advantage in cyberspace.</p>	www.cabinetoffice.gov.uk
2. Centre for the Protection of the National Infrastructure (CPNI)	<p>CPNI is the government authority that provides protective security advice to the national infrastructure. It aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services (delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors) safer.</p> <p>CPNI advice is targeted primarily at the Critical National Infrastructure (CNI) - those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. Without these key elements, the essential services could not be delivered and the UK could suffer serious consequences, including severe economic damage, grave social disruption, or large-scale loss of life.</p>	www.cpni.gov.uk
3. Department for Business, Innovation and Skills (BIS)	<p>BIS has policy responsibilities on several NIS-relevant domains, as for example:</p> <ul style="list-style-type: none"> • Information Security • E-commerce • Electronics and IT services <p>Note that the Digital content, the Telecommunications sector policy and International ICT policy areas are now the responsibility of the Department for Culture, Media and Sport (DCMS).</p>	www.bis.gov.uk
4. Communications-Electronics Security Group (CESG)	<p>CESG is the Information Assurance (IA) arm of GCHQ and is the UK Government's National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing to help our customers achieve their business aims.</p> <p>CESG aims to protect and promote the vital interests of the UK by providing advice and assistance on the security of communications and electronic data. CESG delivers information assurance policy, services and advice that government and other customers need to protect vital information services. CESG works on a cost recovery basis for all customer-specific solutions and services, though IA policy and Guidance documentation is usually free of charge to the UK official community.</p>	www.cesg.gov.uk

National authorities	Role and responsibilities	Website
5. Ofcom	<p>Ofcom is the independent regulator and competition authority for the UK communications industries and has the primary duty to further the interests of citizens and consumers in communications matters. To this end, regulatory interventions are implemented to safeguard access and inclusion in digital communications, particularly where they involve the most disadvantaged sections of society.</p> <p>Ofcom's work both complements and reinforces that of government, as well as the voluntary and private sectors. Using evidence and analysis, Ofcom helps to shape the future regulatory framework, both in the UK and the EU.</p>	www.ofcom.org.uk
6. Information Commissioner's Office (ICO)	<p>The Information Commissioner's Office (the "ICO") is the UK's independent authority set up to promote access to official information and to protect personal information.</p> <p>Its main functions are educating and influencing (promote good practice and give information and advice), resolving problems (resolve eligible complaints from people who think their rights have been breached) and enforcing (use legal sanctions against those who ignore or refuse to accept their obligations).</p> <p>The data protection powers of the ICO are to:</p> <ul style="list-style-type: none"> • conduct assessments to check organisations are complying with the Act; • serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period; • serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law; • prosecute those who commit criminal offences under the Act; • conduct audits to assess whether organisations processing of personal data follows good practice; and • report to the Parliament on data protection issues of concern. 	www.ico.gov.uk
7. Cyber Security Operations Centre (CSOC)	CSOC was established by 2009 Cyber Security Strategy. With an initial staff of 19 and funded from GCHQ's budget, it is co-located with GCHQ's Cheltenham Headquarters.	www.gchq.gov.uk
8. Serious Organized Crime Agency (SOCA)	The Serious Organized Crime Agency (SOCA) is an executive, non-departmental public body sponsored by, but operationally independent of, the Home Office. SOCA is an intelligence-led agency with law enforcement powers and harm reduction responsibilities. Harm in this context is the damage caused to people and communities by serious organised crime.	www.soca.gov.uk
9. Police Central e-crime Unit (PCeU)	Aims to improve the police response to victims of e-crime by developing the capability of the Police Service across England, Wales and Northern Ireland, co-ordinating the law enforcement approach to all types of e-crime, and by providing a national investigative capability for the most serious e-crime incidents	www.met.police.uk/pceu/index.htm

Computer Emergency Response Teams (CERTs)

The below table provides an overview⁵⁴ of the UK's most active CERTs:

CERT	Role and responsibilities <ul style="list-style-type: none"> FIRST⁵⁵ member TI⁵⁶ listed 	Website
10. BP DSAC - BP Digital Security Alert Centre	FIRST member	http://digitalsecurity.bp.com
11. BTCERTCC	FIRST member, TI accredited	www.bt.com
12. CITIGROUP (UK)	Financial Sector CERT, TI Listed	www.trusted-introducer.org/teams/teams-c.html#CITIGROUP
13. CSIRTUK	Government & Military, national / governmental CERT, TI Listed, FIRST member	www.cpmi.gov.uk
14. DAN-CERT - DANTE Computer Emergency Reponse Team	Research & Education CERT, TI Listed, FIRST member	www.dante.net/sf/
15. DCSIRT - Diageo CSIRT	TI Listed, FIRST member	www.diageo.com
16. ECERT - Energis Squared Limited CERT	TI Listed, FIRST member	http://cert.energis2.net/
17. ESISS	TI Listed Constituency: ISP Customer Base	www.esiss.ac.uk
18. EUCS-IRT	TI Listed Constituency: Research & Education	https://www.trusted-introducer.org/teams/teams-e.html#EUCS-IRT
19. GovCertUK - CESGs Government Computer Emergency Response Team	TI Listed Constituency: Government & Military, national / governmental CERT	www.govcertuk.gov.uk
20. JANET CSIRT	TI Accredited, FIRST member Constituency: Research & Education	www.ja.net/csirt
21. MLCIRT (UK)	TI Listed, Financial Sector CERT	https://www.trusted-introducer.org/teams/teams-m.html#MLCIRT
22. MODCERT – Ministry of Defence Computer Emergency Response Team	TI Listed, FIRST member Constituency: Government & Military	www.mod.uk/cert/
23. OxCERT - Oxford University IT Security Team	TI Listed Constituency: Research & Education	www.ict.ox.ac.uk/oxford/com_psecurity/oxcert/
24. Q-CIRT - QinetiQ Computer Incident Response Team	TI Listed, FIRST member Constituency: Major Service Provider	www.qinetiq.com
25. RBSG-ISIRT - Royal Bank of Scotland Group Information Security Incident Response Team	TI Accredited, FIRST member Constituency: Financial Sector	www.rbs.co.uk
26. RM CSIRT (ROYAL MAIL CSIRT CC)	FIRST member	www.first.org/members/teams/rm_csirt/

⁵⁴ See also: ENISA "Inventory of CERT activities in Europe" available since 2011 at:

<http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe>

⁵⁵ See: www.first.org/members/teams/

⁵⁶ See: www.trusted-introducer.nl

WARPs (Warning, Advice and Reporting Points)

WARP	Role and responsibilities	Website
27. NEGWARP	Local Government WARP. The North East regional Local Authority WARP provided by SOCITM North East. Registered September 2009.	N/A
28. NWWARP	Local Government WARP. The North West regional Local Authority WARP, run by the NLA WARP. Registered February 2010.	N/A
29. YHWARP	Local Government WARP. The Yorkshire and Humber regional Local Authority WARP provided by SOCITM Yorkshire and Humber. Registered July 2009.	www.yhwarp.net
30. EMGWARP	Local Government WARP. The East Midlands Government WARP for local authorities in the East Midlands Region of England. Registered June 2006.	www.emgwarp.org
31. WMCWARP	Local Government WARP for Local Government and associated public sector bodies within the West Midlands run by West Midlands Connects. Registered September 2006.	www.necpc.org.uk
32. CY2WARP	Local Government WARP. The Welsh regional Local Authority WARP provided by SOCITM Cymru. Registered July 2009.	www.cymruwarp.net
33. EEWARP	Local Government WARP. A regional Local Authority WARP for the East of England and surrounding authorities provided by SOCITM East of England. Registered July 2009.	www.eewarp.net
34. LCWARP	Local Government WARP. Information Security for London (ISfL), run by Capital Ambition, is the WARP for the London boroughs and associated public sector organisations. Registered April 2003.	www.londoncouncils.gov.uk/capitalambition/projects/isfl.htm
35. SEGWARP	Local Government WARP. The South East Government WARP (SEGWARP) provided by South East Employers for local authorities in the South East of England.	www.seemp.co.uk/index/evenetsnet/segwarp.htm
36. SWWARP	Local Government WARP. The South West regional Local Authority WARP provided by SOCITM South West. Registered May 2007. Registered July 2009.	www.swwarp.net
37. Scotland WARP	Currently there is not a WARP for Local Authorities in Scotland – this WARP is planned.	N/A
38. Northern Ireland WARP	Currently there is not a WARP for Local Authorities in Northern Ireland – this WARP is planned.	N/A
39. CY1WARP	Public Services WARP for the Welsh Assembly and Government in Wales, provided by EADS DS UK Ltd. Registered April 2009.	www.waleswarp.org.uk
40. MODWARP	Public Services WARP. MOD Alerting Warning and Reporting (AWR) structure consists of the Joint Security Co-ordination Centre (JSyCC) the overall controlling WARP with a total of 15 Sub WARPs, as well as being the central WARP for List X and Defence Industry partners, which report on all Information Assurance/Computer Network Defence matters within their respective areas of responsibility. Registered Jan 2008.	N/A
41. NHSWARP	Public Services WARP for the NHS Community, initially in the Midlands Region.	www.wmnhsward.org.uk
42. PoiWARP	Public Services WARP. The Police WARP provided by NPIA (National Policing Improvement Agency) for UK police forces and agencies. Registered Jan 2005.	N/A
43. NUWARP	Registered April 2010, a Digital Security & Governance WARP (NUWARP) provided by the School of Computing, Engineering & Information	N/A

WARP	Role and responsibilities	Website
44. LS1WARP	Sciences at Northumbria University for SMEs. This business WARP is aimed at a small community within The Law Society's membership centred in London. Pending.	N/A
45. TGRWARP	Businesses WARP for the Tigerscheme members (penetration testers). Pending.	www.tigerscheme.org
46. RAYWARP	The Radio Amateurs' Emergency Network – aka RAYNET WARP – this is a voluntary organisation. Registered April 2006.	N/A
47. GUWARP	The Guild WARP (GUWARP) for online members of the Guild of One-Name studies - a Genealogy Society. Registered Jun 2004 - this is a voluntary organisation.	

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
48. Electronic Communications Resilience and Response Group (EC-RRG)	<p>Promotes the availability of electronic communications infrastructure for the UK and provide an industry emergency response capability through the ownership and maintenance of the National Emergency Plan for Telecoms.</p> <p>EC-RRG is chaired by an industry representative and hosted by BIS (the Department for Business Innovation and Skills). EC-RRG takes the lead in developing and maintaining co-operation between the telecommunication industry and government through:</p> <ul style="list-style-type: none"> • Providing a forum for exchanging information between industry experts in telecommunications resilience and those parts of government with a policy interest in resilience • Planning (including ownership of the National Emergency Plan for the Telecommunications Sector) and • Providing a response capability to emergencies through NEAT, (the National Emergency Alert for Telecommunications). 	interim.cabinetoffice.gov.uk
49. OWASP - The OpenWeb Application Security Project	The OpenWeb Application Security Project (OWASP) is the leading source of information, guidance and tools on web application security. OWASP has over 130 local chapters worldwide, with three in the UK - London, Leeds and Scotland.	www.owasp.org
50. British Computer Society - Information Security Specialist Group (BCS-ISSG)	ISSG is a specialist sub-group of BCS. ISSG's objective is to raise awareness of risks to information systems and identify technical and non-technical methods for attaining acceptable levels of security	www.bcs.issg.org.uk
51. Information Security Awareness Forum	The Information Security Awareness Forum to coordinates and build on existing work and initiatives, to improve their overall effectiveness, and ultimately to increase the level of security awareness in the UK. The forum was launched on the 13th February 2008. The member representatives meet twice a month to progress the agenda and actions of the forum.	www.theisaf.org
52. tScheme	The tScheme initiative became an independent limited company in May 2000. Its members have contributed to the successful development and implementation of an objective, transparent,	www.tscheme.org

Industry Organisations	Role and responsibilities	Website
	proportionate, and non-discriminatory scheme for trust services industry self-regulation, within the context of the EC Directive 1999/93/EC 'Electronic Signatures.'	
53. The UK Technology Industry (Intellect)	Intellect is the trade association for the UK technology industry. It provides a voice for its members (800 companies ranging from SMEs to multinationals) and works in both markets and policy fields including the Data Breach Notification Working Group, the Defense and Security Commercial Council, the Digital Communications Market Group, the Identity Management Working Group, the Security and Privacy Group, and the Security and Resilience Group.	www.intellectuk.org
54. British Security Industry Association (BSIA)	BSIA disseminates information to members, potential members, users of security products/services, related organizations and the general public to raise awareness and understanding of issues relating to security and crime prevention. It draws up industry codes of practice and technical documents.	www.bsia.co.uk
55. Mobile Industry Crime Action Forum (MICAF)	<p>The Mobile Industry Crime Action Forum is a forum for the exchange of information and the promotion of a united effort against criminal activity in telecommunications.</p> <p>The Forum seeks to raise awareness of crime issues affecting the industry or impacting on its customers and suppliers. It helps identify and develop counter-measures to telecom crime as well as develops procedures to combat mobile phone related crime in UK.</p>	www.micaf.co.uk

Academic organisations active in network and information security

NOTE: due to the very high number of UK academic organisations with activities in the NIS domain only a very limited list was included below.

Academic Organisations	Role and responsibilities	Website
56. Institute for Information Security Professionals (IISP)	<p>The principal objective of the Institute is to advance the professionalism of information security practitioners and thereby the professionalism of the industry as a whole. The Institute aims to provide a universally accepted focal point for the information security profession.</p> <p>The Institute is an independent not-for-profit body governed by its members, ensuring standards of professionalism - for training, qualifications, operating practices and individuals.</p>	www.instisp.org
57. Royal Holloway University of London	Royal Holloway is a multi-faculty college of the University of London. Its Information Security Group is one of the largest academic security groups in the world. It brings together in a single institution expertise in education, research and practice in the field of information security	www.isg.rhul.ac.uk

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
58. Cyber Security Challenge UK	<p>Cyber Security Challenge UK Limited has recently been set up as a not for profit company to address reported problems in the UK about:</p> <ul style="list-style-type: none"> • the difficulty of recruitment to cyber security jobs, • predictions about an increase in the number of cyber security jobs and • a decrease in the number of people applying to fill cyber security jobs. 	https://cybersecuritychallenge.org.uk
59. ISACA (Information Systems Audit and Control Association) – UK Chapter	ISACA is an organization for information governance, control, security and audit professionals.	www.isaca.org/uk
60. British Standards Institute (BSI)	BSI, the UK's national standards body, certifies management systems and products; provides product testing services; develops private, national and international standards; provides training and information on standards and international trade; and provides performance management software solutions. It specifically addresses information security and IT network security.	www.bsi-global.com
61. ISCA	Part of the European 'Insafe' Internet safety network under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children. Its goal is also to fight against illegal content and content unwanted by the end-user. The initiative is part of the EU's coherent approach.	www.internetsafetyzone.co.uk
62. BCS Security Forum	<p>BCS members can participate in discussions at the new security forum discussion area.</p> <p>The aim of the BCS Security Forum is to be a catalyst for change within the ICT and information security community. These forums have been set up as another way of increasing the impact and recognition of IT professionals. They complement the work of other successful groups within BCS such as the specialist groups and branches and aim to provide a mechanism by which members can understand and influence their sector of interest at the highest level.</p> <p>The security community is diverse, and its influence wide-ranging, but its effectiveness can only be enhanced if it speaks with a single, authoritative voice on matters of importance to the citizen, business, commerce and government.</p>	www.bcs.org
63. Information Assurance Advisory Council (IAAC)	IAAC's mission is to advance information assurance to ensure the UK information society can count on a robust, resilient, and secure foundation. The IAAC is a partnership that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. It makes policy recommendations to government and corporate leaders at the highest levels. IAAC's sponsors and members comprise leading commercial end users, government policy makers, and the research community. IAAC's aim is to work for the creation of a safe and secure information society.	www.ktn.qinetiq-tim.net

References

- ENISA "Inventory of CERT activities in Europe" available at: <http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe>
- 2010 UK National Security Strategy document 'A Strong Britain in an Age of Uncertainty' at www.direct.gov.uk
- 2010 UK Strategic Defence and Security Review document at www.direct.gov.uk
- Study on eID Interoperability for PEGS: Update of Country Profiles - <http://ec.europa.eu/idabc/servlets/Docb482.pdf?id=32522>
- UK Security Policy Framework (SPF) at <http://www.cabinetoffice.gov.uk/spf>
- The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010
- The 2008 Information Security Breaches Survey (the main Technical Report and the Executive Summary) is available to download or order from www.security-survey.gov.uk
- UK WARP directory at: www.warp.gov.uk/directory.html
- UK National Emergency Plan for Telecommunications document, available at: <http://interim.cabinetoffice.gov.uk/media/418987/nep-telecomms-sector-march2010.pdf>
- The post exercise public report of the Exercise White Noise available at: <http://interim.cabinetoffice.gov.uk/media/427527/bis-exercise-white-noise.pdf>
- "Traffic Management and 'net neutrality'" document published by Ofcom at: <http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf>
- See the full version of the published by the House of Lords, European Union Committee - Fifth Report Protecting Europe against large-scale cyber-attacks, at: <http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6802.htm> . Ordered to be printed 9 March 2010 and published 18 March 2010.
- The June 2009 version of the UK Cyber Security Strategy at: http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

