



www.ddsi.org

National Dependability Policy Environments

UNITED KINGDOM

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: King's College London (UK)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country’s Information Infrastructure 3
Main ICT Regulatory and Legal Developments 4
Assessment of Phenomena Undermining Dependability 6
Government Initiatives Aimed at Tackling Cyber Issues..... 8
Industry and Other Non-Government Activities Related to Dependability 11
Public-Private Partnerships 13
Research and Development 14

Overview of the Country's Information Infrastructure

Use of IT in the UK has grown steadily since the 1960s with overall ICT penetration in businesses rising to 80 PCs per 100 white collar workers by 1999. 25% of the workforce had Internet access by 2001. The business 'take-up' of IT has seen 83% having their own web-site in the same timeframe. PC penetration in the UK has continued at a steady rate for the last few years and in 2000 the IT market expanded by 12.7%, in 2001 by 11.8%. By 2001, some 9m internet users (average number of active users, 1.41 per household) resulted in over 27% of the population being on-line and of these about 30% used the systems for e-commerce or banking-on-line.

It has been widely accepted that consumer demand is the driving force behind IT hardware purchases. As more and more consumers are connected to the Internet, so businesses are having to invest in more or better technology to keep up with demand. Figures at the end of December 2001 revealed that around 10m people visited shopping web-sites in the UK in November 2001; this was an increase of 900,000 from the same period in the previous year. This indicates that overall, the number of people making secure purchases has increased. Figures for November were an increase of 11% on those for October 2001.¹

Other major drivers for the ICT market were the decreasing total cost of ownership for IT hardware (both in the business and household sectors) and steadily decreasing prices. 2000 also saw the explosion of the ASP (Application Service Provider) market as many companies chose to outsource their IT functions to third party companies, using software as a service delivered over the Internet. Other IT drivers have been CRM (Customer Relationship Management), ERP (Enterprise Resource Planning) and SCM (Supply Chain Management). CRM has proved to be particularly popular and the government is embarking on a number of CRM projects as part of its raft of G2C (Government to Citizen) services.

For a number of reasons, the UK is significantly more dependent than the rest of Europe on ICT environments that require a highly skilled workforce. Reasons for high demand for ICT skills may include the fact that English is the language of the Internet, the high presence of US companies with regional headquarters in Europe and the large services and banking sectors based upon the 'global time-zone' and 'geographic positioning' of the UK. It was expected that the ICT skills shortage would increase to 291,800 in 2001. The shortfall in labour has been offset by the use of Indian-Sub Continent contracted personnel functioning during the UK 'night', thereby allowing a 24x7 operation. Consideration is being given to allowing IT skilled 'economic migrants' to settle under 'green card' schemes.

A rise in on-line services for travel, insurance etc., has resulted in the new 'call-centre' industry. Such centres are frequently established in 'depressed' towns or regions but service a global English speaking audience.

As of mid-2000, mobile phone penetration was at 54% of the population,; this has been rising ever since. It is expected that this will slow to between 70 and 80% of the population in the years 2002 – 2005. Whilst the growth rate was 35% in 2000, in the years 2001 – 2005 it is expected to fall as the market

¹ NUA Internet Surveys Dec 21 2001, available at http://www.nua.com/surveys/index.cgi?f=VS&art_id=905357512&rel=true (visited on 21 March 2002)

reaches saturation point.² The UK also saw incredible growth of value added services like SMS (Short Message Service). WAP (Wide Area Protocol) services have so far failed to take off as expected. However, increasing competition (like the entrant into the market of a fifth service provider, 'Fresh') and more effective regulation, (as knowledge of the sector increases) have resulted in decreasing prices.

In 2000 the auction of 3G (UTMS) mobile licenses took place. Five consortia were eventually given licenses out of 13 applicants, but the high prices paid for each licence may result in further investments to improve the infrastructure being delayed.

The take up of ADSL (Asynchronous Digital Subscriber Line) broadband has been very slow. The UK has 0.3% of its lines converted to DSL, which is behind every country in Europe except for Greece, Portugal, Ireland and Luxemburg. Government has made several promises that Britain would become the most competitive broadband market and has established a Broadband Stakeholders Group to drive forward roll-out but it seems unlikely that the UK will meet its target of becoming the most competitive broadband market in the G-7 by 2005, given that the country is at present in last place.³

Main ICT Regulatory and Legal Developments

The UK's approach to the Information Society was laid out in its 1998 Competitiveness White Paper that noted the major role played by ICT in facilitating growth and set the goal of "making the UK the best environment in the world for e-commerce." In September 1999 the Cabinet Office issued ecommerce@its.best.uk.⁴ This report laid out the organisational and policy framework for achieving these goals.

The UK philosophy was outlined by the Prime Minister:

"Countries that wholeheartedly embrace e-commerce will benefit from improved national economic performance. Those that do not risk seeing trade ebb away to low cost competitors elsewhere in the world. ...

[we have] identified three areas in which we need to make progress – we need to facilitate access to the technology and networks, we need to enhance understanding of the potential of e-commerce and we need to create an environment where people can have trust in the new medium. There are some things Government can do. For example, we need to ensure that all sections of society have the opportunity to share in the benefits of the e-commerce revolution. We have also got to give a higher political priority to electronic commerce ...

But it is clear that the Government alone cannot drive forward the development of e-commerce. What is needed is a sustained joint campaign between Government and business to ensure that we reap the benefits. Similarly, Government cannot simply regulate to achieve its aims in this new global electronic environment. This report, therefore, recommends a light regulatory touch. Enough to build confidence in the new way of doing business and to protect consumers, but not so much that we stifle innovation, creativity and entrepreneurship and drive industry overseas."

² http://www.mobilecomms-technology.com/projects/gprs_uk/gprs_uk1.html, (visited on 21 March 2002)

³ 'Broadband: its time for action' *Computing*, 22nd November 2001

⁴ <http://www.cabinet-office.gov.uk/innovation/1999/ecomms.shtml> (visited on 21 March 2002)

Whilst the overall strategy has been delineated by the Prime Minister, the regulatory approach to make this a reality has been hampered by opposing views of the two main government departments involved: the Home Office and the Department of Trade and Industry. The Home Office, which has crime prevention as its remit, has the view that the Internet and e-Commerce needs to be regulated heavily to protect citizens and consumers. The Department of Trade and Industry, on the other hand, has taken a view consistent with the G-8 principles of regulation of the Internet, i.e. minimal regulatory intervention to allow the market to flourish as much as possible. This dichotomy has resulted in a number of differences between government departments and a sometimes confusing e-Commerce environment.

Notwithstanding these intergovernmental differences, the UK economic and industrial environment related to ICT has developed at a quite rapid pace. Since the 1980s, the UK has undertaken an extensive programme of market liberalisation and privatisation. Combined with London's status as a world capital for the financial industry and services sector, this process of deregulation put the UK in a good position to exploit the technology boom in the late 1990s. The ICT contribution to UK GDP has been rising albeit only slowly, from 6.37% in 1997 to 7.4% in 2000. However the ICT manufacturing and services trade has shown considerable expansion even taking into account inflation. In 1998 it was 79,286m EUROS and by 2001 had reached 112,125m EUROS.

In 2000 the auction of 3G (UTMS) mobile licenses took place which netted the government 54bn EUROS from the five winning consortia. The licenses contain an obligation to build a network to cover at least 80% of the population by the end of 2007. Frequency bands have been adjusted to allow greater commercial bandwidth. Digital services are increasing so that homes and offices have multiple pathways to receive or even send information.

The British government is particularly concerned by the need to foster the take-up of ICT services and functionalities by SMEs and the educational sector. In the 2000 budget, the Chancellor Gordon Brown introduced a special tax cut to encourage Small & Medium Enterprises (SME's) to go on-line. 100% of the cost of new information technology or e-Commerce investments can be written off against tax. This policy seemed to have worked. Only 2% of UK businesses are not on-line, and 17% do not have some form of World Wide Web presence. UK Online for Business has been undertaking an educational and awareness campaign encouraging businesses, especially SMEs, to get on-line. The network of *Business Links* provide advice and training at the local level.

E-Government is also playing a fundamental role in the activities of the British government. The recommendations of ecommerce@its.best.uk have been implemented under a national strategy known as UK Online. The UK Online Annual Reports provide comprehensive updates on progress.⁵ The 2nd annual report by UK Online, published in December 2001, indicates that the UK is underachieving in its ambitious ICT goals. The report notes that fifty three of the 94 recommendations that were due to be completed in 2000 have not been fully achieved.

The report made much of the fact that UK e-government structures are some of the most advanced in the world, but downplayed other issues like the poor levels of infrastructure provision for next generation internet services (e.g. broadband). Although the e-Envoy, Andrew Pinder, pointed out that 74% of all government transactions will be on-line by next year, an information society lobbying group, Eurim, has said that the government's goal of getting all government services on-line by 2005 is 'doomed to fail'. Other surveys have consistently placed the UK behind many other industrialised countries in the e-

⁵ http://www.e-envoy.gov.uk/ukon-line/champions/anrep_menu.htm

Commerce league. Notwithstanding these difficulties, central government is committed to deliver 100% of its services electronically, through the telephone, computer and/or TV by 2005. One key component of the IAG project is the Government Secure Intranet (GSI). This is intended to provide electronic connectivity between government departments and agencies. The GSI provides Internet access but also has a variety of related components that operate at higher levels of security. Effectively operational since the end of 1998, the rapid take-up of the GSI can be seen in the fact that the number of users rose from under 17,000 in June 1999 to over 90,000 at the end of the year.

Notwithstanding all of these initiatives, the success of the British information society will come from an appropriate regulatory framework for the provision of information and communication services. The achievement of this objective may lead to government-industry conflicts as in the case of the Regulation of Investigatory Powers Act (RIPA) and the Electronic Commerce Act (ECA). Broadly speaking, RIPA was criticised for being too heavily focused on aspects of criminality, which is unsurprising given that it was backed by the Home Office. Ministers had much difficulty in refuting many of the claims made against the government by privacy advocates and businesses, who argued that not only did it reverse the burden of proof in several areas (thus constituting a infringement of human rights) but it would also cost UK ISPs around £46bn to make their network infrastructures compatible with the interception requirements of the Act.

On the other hand, the Electronic Commerce Act (ECA) was backed by the Department of Trade and Industry (DTI) and showed a desire to adopt a minimal regulatory approach in order to foster the market. The Act concerned the adoption of digital signatures in the United Kingdom and the provision of certification authorities. Electronic signatures are legally admissible in court as evidence and are binding in contracts. The Act also allows for the approval of cryptography providers by the Secretary of State. Importantly, a system of public key escrow was prohibited by this act (a principle which seemed to be contradicted by the tone of the RIPA).⁶

Assessment of Phenomena Undermining Dependability

The paucity of reliable data on the state of information security and factors affecting dependability poses real difficulties to British policy makers. Whilst anecdotal evidence and surveys of limited samples are easy to come by, there is no certainty that such sources provide useful data on which to base policy. Exaggerated claims from the information security industry serve only to muddy the waters.⁷ While anecdotal evidence should not drive policy formulation, high-profile breaches of cyber-security do have an impact on the perceptions of the public, businesses and policy-makers. Recent incidents that have made headlines include:

- In July 2000, 'Herbless' (the handle of a still unidentified hacker) attacked a number of British web-sites, including several government sites, HSBC and the Cabinet Office.⁸
- In the middle of 2000 Powergen, a UK utilities company was found to have a massive breach in its web server. A customer was able to download the entire database of debit card details of thousands of customers.

⁶ <http://www.bmck.com/ecommerce/uk.htm#ecb> (visited on 21 March 2002)

⁷ 'Hacking Contest Publicity Stunt Backfires', The Register, 1st May 2001 available at <http://www.theregister.co.uk/content/8/18499.html>

⁸ <http://www.sans.org/infosecFAQ/hackers/herbless.htm>, (visited on 21 March 2002)

- In January 2001, the UK government acknowledged that in September 1999 a security guard at the Bradwell Nuclear Plant attempted to hack into the plant's computer system. The entire plant was locked down to conduct a security review.⁹
- The Welsh teenager Raphael Gray stole more than 26,000 credit card numbers from servers across the globe.
- The National Criminal Intelligence Service reported that over 50% of frauds investigated in the first six months of 2000 were computer-related.
- NCIS's 1999 *Project Trawler* estimated that computer crime in the UK was growing at an annual rate of 7.4%.
- A 2001 KPMG survey reported that the UK is the "worst country in the world for cyber-crime", where 14% of respondent companies had been hacked.¹⁰

The 2002 KPMG Information Security Breaches Survey has confirmed the increasing incidents of information security breaches among British companies. It was remarked that security breaches are in the increase as "44% of the UK businesses have suffered a security breach during 2001 (with 78% of large businesses suffering a breach). The survey also examined how companies perceived the seriousness of security breaches. The survey remarked that "in terms of severity, 79% of UK businesses that had security incidents in the last year had at least one that they rated serious, and 20% stated that they had extremely serious incidents. The larger the business the less likely that a single security incident was considered serious. Only 56% of large businesses that had security incidents in the last year had at least one that they rated serious".¹¹

The Department of Trade & Industry has concluded that, "security concerns are holding back widespread adoption of the internet as the primary business communication medium."¹² The Cabinet Office's Performance and Innovation Unit has concluded that some 75% of retail consumers are concerned about privacy on-line. Similarly, some 90% of corporate executives believe that security is a key enabler for the growth of e-business.¹³

⁹ 'N-station security to be increased after hacking bid' Ananova, 09th January 2001 available at http://www.ananova.co.uk/news/story/sm_166187.html, (visited on 21 March 2002)

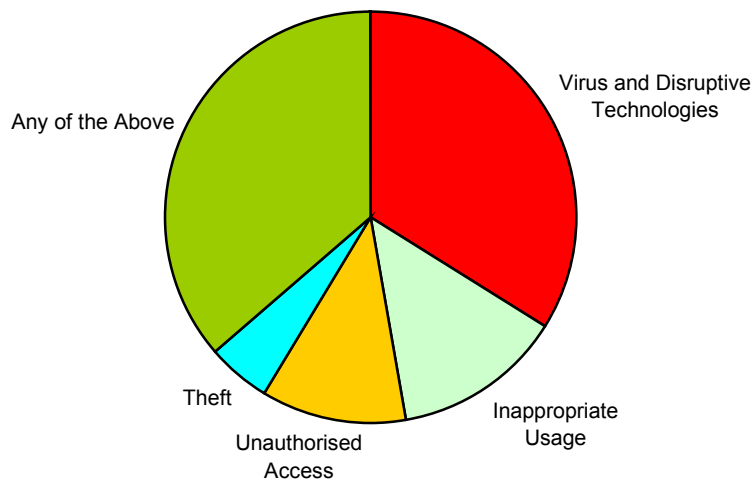
¹⁰ PCB Solicitors, *The Fraud Prevention Report*, Summer 2001

¹¹ DTI/KPMG, *Information Security Breaches Survey, 2002-Technical Report*, April 2002.

¹² InterForum: White Paper "Electronic Signatures—signing up to the Digital Economy"

¹³ www.dti.gov.uk/cii/dtigreen/dti_site_site/index.htm (visited on 21 March 2002)

**What Proportion of UK Businesses Suffered Security
Incidents in the Last 12 Months**
(Source: KPMG-DTI Survey 2002)



Government Initiatives Aimed at Tackling Cyber Issues

Since the end of WWII, United Kingdom internal security has been focused towards physical protection primarily as a result of the problems in Northern Ireland that, from time to time, have spilled over into indiscriminate attacks on mainland Government and civilian sites. Well exercised procedures exist for emergency planning and contingency measures designed to protect sensitive areas, handle resulting casualties and thereafter restore services. The external threat was perceived as coming from the Warsaw Pact nations who engaged in 'intelligence collection' through a spectrum of attacks targeted against the UK.

The Government and 'List X companies' operated computing systems in accordance with standards advised by the Communications Electronic Security Group. This evolved into ITSec standards that became the Common Criteria and were accepted by many western nations.

On two occasions in the past year, HM ministers have addressed cyber-risk. Then Foreign Secretary Robin Cook told Parliament on 29 March 2001 that "a computer-based attack on the national infrastructure could cripple the nation more quickly than a military strike."¹⁴ In February 2001, then Home Secretary Jack Straw had told the BBC that "the results of cyber-terrorism, by which people could hack into the control systems of, say, the water supply, the electricity supply, those operating a hospital could be worse even than those caused directly by explosion.

Whilst the Government encouraged all in the UK to take effective action for Y2K, it was actually late in comparison with many major corporations who had commenced programmes at least twelve months ahead of HMG. Fortunately Y2K passed without any major incidents but lessons have been learned. In February 2000, then Leader of the House Margaret Beckett, who had coordinated government preparations for Y2K, made these concerns explicit, arguing that: "Information Infrastructure Protection

¹⁴ Hansard, 29 March 2001

- keeping our 'phones, power, utilities, finance, transport, Government safe and protected - is the new challenge for this Millennium."¹⁵

The adoption of new Critical National Infrastructure (CNI) paradigms, for instance that of "national resilience" indicates a recognition on the part of government that lessons from non-cyber crises (e.g. fuel protests, 11 September, foot and mouth) need to be incorporated into an understanding of systemic risks to the Information Society. Terrorism, Law & Order, and continuity of public services have been traditionally under the Home Office.¹⁶ Commerce fell under the remit of the Department of Trade & Industry. The movement of Utilities and other nationalised key infrastructures away from government control into the privatised sector has left their 'protection' stretched across varying Departments. In relation to IA and protection of critical information infrastructures, the overall approach of the Blair government has continued to be influenced by non-interventionism. This has meant a preference for market solutions that are both implemented and paid for by the private sector.

The Cabinet Office has evolved under the current political administration into a more centralising co-ordination policy role, maintaining an overview across the wider administrative spectrum.¹⁷ In 2002, the e-Envoy, who reports directly to the Prime Minister was made the national "sponsor" for Information Assurance. He is now developing a national strategy to coordinate policy and reach out to the private sector. The e-Minister provides political leadership across Government in driving forward the Government's objectives on e-commerce and has particular responsibility for delivery of e-Government objectives.¹⁸

One of the Cabinet Committees is the Civil Contingencies Committee (CCC) composed of Secretary of State for the Home Department and others, including the Cabinet Office, Treasury and the devolved administrations, who are invited to attend, depending on the contingency. Its Terms of Reference are "to co-ordinate the preparation of plans for ensuring in an emergency the supplies and services essential to the life of the community; to keep these plans under regular review; and to supervise their prompt and effective implementation in specific emergencies." The Committee is supported by the Civil Contingencies Secretariat (CCS), set up in 2001 to coordinate national resilience and management of societal risks.

Within the Cabinet Office, the Security Division exists to support the relevant Cabinet official committees in developing protective security policy. This includes promoting best practice, issuing guidance and providing advice across government and to associated bodies. These responsibilities cover all aspects of protective security policy including personnel, physical, document, IT and communications security. The policy framework on protective security applies to all Government departments and agencies, and also to private sector contractors who have access to sensitive material, but each department and agency is responsible, under Ministerial direction, for maintaining its own security regime. The Division is responsible for promoting ISO17799 within Government, and supports departments in ensuring compliance with the standard. The Security Division also supports the work of the National Infrastructure Security Co-ordination Centre (NISCC), the interdepartmental organisation set up to co-ordinate and develop existing work within Government departments and agencies, and organisations in the private sector, to defend the UK's critical infrastructure against electronic attack.

¹⁵ CESG / HSA Conference, 22nd Feb 2000, Protecting the National Information Infrastructure, London.

¹⁶ <http://www.homeoffice.gov.uk> (visited on 21 March 2002)

¹⁷ <http://www.cabinet-office.gov.uk/> (visited on 21 March 2002)

¹⁸ <http://www.e-envoy.gov.uk> (visited on 21 March 2002)

NISCC operates under a Director, who is a member of a Management Board chaired by the [Home Office](#).¹⁹ Other members of the Board are drawn from the [Cabinet Office](#), the [Communications-Electronics Security Group \(CESG\)](#) of [GCHQ](#), the [Security Service](#), the [Ministry of Defence](#) and the Police. NISCC is responsible for co-ordinating the dialogue with owners of CNI systems, collect alerts and warning of attacks and provide assistance for serious attacks.

The National Hi-Tech Crime Unit was established in 2001 as part of the government's commitment to developing a national hi-tech crime strategy. The Unit is responsible both for dealing with serious cyber-crimes and building capacity in regional police forces. The Unit is now experimenting with confidential reporting systems to build better relations with industry.

The Unit is supported by the Home Office's hi-tech crime research programme. Initially, a prime objective is to determine the nature and impact of hi-tech crime in the UK. Based on available literature, audits and surveys, this project is a foundation study to define hi-tech crime and describe its scope, nature and impact within the UK. The study will produce an overview of what is known about hi-tech offenders, victims, fear of hi-tech crime, crime types and consequences. The study will make recommendations to assist the development of policy practice in the area, and will identify future research priorities.

Notwithstanding all of these initiatives, the Government has taken a "light touch" approach to promoting consumer confidence and trust in e-Commerce. This has been commended by the Better Regulation Task Force which argues that "Government should not interfere with the development of self-regulatory schemes but should allow the market to develop."²⁰ Direct Government regulation has focused on the area of data protection, with the Information Commissioner encouraging the private and public sectors alike to comply with the legislation at the same time as promoting self-regulatory schemes.

Considerable basic security advice is available within different government web-sites, but these require a degree of positive research rather than a set of hyperlinks that encompass the full breadth of knowledge and support that might be available to industry or the private citizen. An example of Government and limited non-government access to information on cyber-attacks is the Unified Incident Reporting and Alert Scheme (UNIRAS) which was established in 1992 with the role of gathering information on IT security incidents in Government departments and agencies, producing periodic analysis and assessment of incidents and trends, and issuing alerts and briefings on matters of IT security concern. UNIRAS, now a fully integrated part of the NISCC, has had its role extended considerably in the last two years. Its original customer base of Government departments and agencies has been expanded to include companies holding sensitive government contracts, and most recently Critical National Infrastructure (CNI) organisations. UNIRAS' functions fall into three main categories. First, it provides responses to electronic attacks and other IT security incidents, as well as gathering infosec-related information.

UNIRAS is also the UK Government Computer Emergency Response Team (CERT) and is an active member of the international Forum of Incident Response and Security Teams (FIRST).²¹ UNIRAS provides a real-time help desk and early warning function for its customers. UNIRAS co-ordinates the [NISCC's Electronic Attack Response Group \(EARG\)](#), which responds to serious electronic attack incidents affecting the CNI. The EARG mobilises specialist Government technical, security and

¹⁹ <http://www.nisc.gov.uk/> (visited on 21 March 2002)

²⁰ [Regulating Cyberspace: Better Regulation for e-commerce](#), p. 9.

²¹ <http://www.first.org> (visited on 21 March 2002)

emergency response resources to respond to serious electronic attack incidents. The level of response depends on the severity and scale of the attack.

Whilst the Reporting Scheme is only available for Government and CNI organisations, non-Government and non-CNI organisations can make use of the UNIRAS [Alerts and Briefings](#) that are posted on the UNIRAS web site. UNIRAS also welcomes reports of significant electronic attack incidents, threats or information about new electronic vulnerabilities from organisations outside the UNIRAS community.

Another key input to UK Security comes from CESG ²² which is the Information Security arm of GCHQ. It is the UK government's national technical authority for information security/ information assurance issues. CESG was formally established in 1969 although elements of the organisation had been in operation since the Second World War. It helps formulate information security policy and guidance for official use. The client base is UK government departments and agencies, the armed forces and cross-cutting programmes such as e-Government, and Critical National Infrastructure (CNI) protection with information security/information assurance issues.

The Department of Trade and Industry ²³ provides extensive security guidelines. These guidelines are designed to support managers in assessing the appropriate security measures for their organisation so that the most cost-effective solutions can be applied. Extensive reference is made to security guidelines and standards such as Code of Practice for Information Security Management. BS 7799 or the Information Technology Security Evaluation Criteria (ITSEC).

As with other countries, the United Kingdom has not built upon the knowledge and experience gained in dealing with Y2K. In 1999, the Department of Trade and Industry (DTI) created ACTION 2000, a private company whose objective was to raise awareness among SMEs and other stakeholders of the dangers posed by the Millennium Bug. More importantly, ACTION 2000's main corporate objective was avoid "material disruption" from this software problem. In order to achieve these objectives, ACTION 2000 carried out several initiatives and projects aimed at gaining a detailed understanding of the country's interdependencies among critical infrastructures. A National Infrastructure Assessment Programme was launched. Between 1998 and 1999 consultants from Ernst and Young examined the structure of the national infrastructure and carried a reasoned analysis of where its critical interdependencies lay. A National Infrastructure Forum was also created involving representatives of all elements of national critical infrastructure. Finally, independent and disclosure were carried out forcing public organisations to become Y2K compliant.

As commented by John Naughton, these activities have made the entire experience a success and indicates that "the model of using a private sector organisation to achieve certain kinds of public-sector goals has much to commend it".²⁴ More importantly, "the cost of Action 2000 experiment does not seem disproportionate in terms of the threat and the priority attached by the government".

Industry and Other Non-Government Activities Related to Dependability

The UK business environment is regulated but in 'cyber-security' matters it has been left to its own devices. Indeed there is a powerful argument, notably from business leaders of the "new economy," that

²² <http://www.cesg.gov.uk/> (visited on 21 March 2002)

²³ <http://www.dti.gov.uk> (visited on 21 March 2002)

²⁴ John Naughton, *Public Sector Values/Private Sector Methods: The Story of Action 2000*, p.3

government intervention, especially in the form of regulation, will not help promote cyber-security but may instead hinder the growth of e-Commerce.

Many of the largest private sectors are dominated by multi-national corporations who operate throughout the world, comply with local regulatory requirements but select COTS products for ICT cost effectiveness and similarly, frequently use the best security practices that can be found.

Within the UK, unless covered by CNI status, they are unable to have suitable and current 'threat' information which would allow the correct management of ICT 'risk'. Thus cyber-security investment has to be on a 'wildcard' basis and therefore not specific and best practice. End-users of ICT are increasingly recognising the risks to which they are exposed, including the direct costs of security breaches, legal liabilities from their value chains and from third parties and the costs to corporate reputations. At the same time, they are beginning to identify trust and privacy as a useful market differentiator and enhancer of the corporate brand.

In general throughout UK industry, policy-making and risk management are severely hampered by the lack of information on cyber-threats, incidents and vulnerabilities. The mid-90s saw a plethora of commercial conferences on Information Warfare and cyber-crime as the demand for knowledge grew and was not satisfied by the Government. At many levels, from local Chambers of Commerce and 'Institute' workshops there is a growth and demand for 'information assurance' awareness. Individual national professional, managerial and industry groups have programmes that increase awareness and debate. Frequently these allow for information on 'lessons learnt' or 'attack successes' to be exchanged in non-public/attributional formats.

The Confederation of British Industry (CBI) has taken Information Security as a separate subject as the increased interdependence and integration of different computer systems has brought gains in efficiency, productivity and communication to its membership. The CBI encourages the use of standards such as BS7799, and a greater awareness of information security principles and guidelines across industry. It is driving initiatives to improve awareness of information security, particularly in those companies which are involved in e-business. It further represents its membership interests as a key contributor to the OECD's Information Security Guidelines review, as well as in the EU and Council of Europe.

The British Computer Society (BCS)²⁵ is the only Chartered Engineering Institution for Information Systems Engineering and has many local Branches which promote 'security' amongst its wide range of subjects. However it also offers education and a Certificate in Information Security Management Principles which is designed to provide the foundation of knowledge necessary for individuals who have security responsibility as part of their day to day role, or who are thinking of moving into a security-related function.

The Computing Services & Software Association (CSSA)²⁶ recently launched the Security Alliance for the Internet and New Technologies (SAINT). This is a grouping within the IT Industry to promote awareness and best practices on information security. Initiatives of this type provide important commercial benefits for industry by increasing the demand for 'fit-for-purpose' information security.

²⁵ <http://www.bcs.org.uk> (visited on 21 March 2002)

²⁶ <http://www.cssa.co.uk> (visited on 21 March 2002)

The Institute of Management, Institute of Directors also have sub-groups that organise workshops, seminars and discussion papers to raise their members awareness.

Professional technical bodies such as the IEEE are 'international' in their approach and have an extensive cyber-security and telematics knowledge bank and run courses and workshops throughout the regions.

Most professional institutes now have some level of knowledge/promotion covering cyber-security issues. Mostly, these relate to principles and process rather than specifics.

In addition to the previous activities, the UK has several CERTs/CSIRTs, which serve either defined communities (e.g. JANET – the academic CERT) or their own companies (e.g. BT CERT). Other commercial CERT services are provided by ICT providers as a service to their customer base. In addition, UNIRAS acts as the government CERT as well as providing services to companies within the CNI. UNIRAS provides a passive service to the wider population via its web-sites. It has now initiated a small programme on information sharing and is promoting the concept of WARPs (Warning, Advice & Reporting Points) that can be established by existing communities of interest such as trade associations.

More recent initiatives include the World-Wide ISAC, managed by Global Integrity/Predictive Systems using the same infrastructure as US-based ISACs. The WW-ISAC provides a valued service to its members, who are primarily large financial institutions based in London. At the end of 2001, the CSSA trade association launched SAINT, with assistance from the DTI and advice from the US IT-ISAC. A founding meeting was held in February 2002.

Public-Private Partnerships

Public-Private partnership is a key strategy for Government. In most aspects this is related to 'funding' where commerce invests and takes the risk for managing or operating a public service. In the cyber-security domain the model is less clear. The 'Partnership' is based on traditional trust relationships in major utilities that form the CNI. In order for these sectors to invest in greater security, they are provided with more information to allow a cyber-threat business investment case to be constructed. The UK also has the residue of past 'old boy networks' that enable exchanges of information and 'guidance' to be passed between trusted individuals who have a common bond/aim. These networks may bridge government/industry or act within sectors between 'competing' organisations. As part of the government's wish to improve the state of national cyber-protection without heavy investment, it participates and sometimes actively encourages organisations to band together to raise awareness and provide feedback to government.

The Information Assurance Advisory Council (IAAC), founded some two years ago is a private sector led, cross-sectoral forum dedicated to providing policy recommendations on information assurance. IAAC²⁷ produces policy advice based on professional analysis and global best practice by bringing together corporate leaders, public policy makers, law enforcement and the research community to address the security challenges of the Information Society.

In March 2002, IAAC issued a Manifesto for "Protecting the Digital Society" which called for the Government to: "make plain the strategic significance of the problem, set out national goals in information assurance, provide basic standards, delineate the government's roles, encourage continued business co-operation and information-sharing, and guide international co-operation." In particular, it

²⁷ <http://www.iaac.org.uk> (visited on 21 March 2002)

called for a more coherent, long-term strategy to address information security concerns, devise best practices and improve education and awareness and set a coherent R&D strategy.

Research and Development

The UK has international expertise in dependability-related research and development. Theoretical and applied research is carried out in a number of areas, most notably cryptography, network protocols computer artifact fingerprinting communications reliability computer fraud detection computer security management and privacy policies. At the government level, the most prominent set of research activities are carried out regularly by Government Communication Headquarters (GCHQ). Much applied research is also carried out by Qinetiq, formerly the UK Defence Evaluation Research Agency (DERA). Although this organisation has been privatised, it has kept in-house capabilities in dependability-sensitive areas like anti-virus, network monitoring/intrusion detection, artificial intelligence and adaptive systems.

There are a number of universities that are actively involved in dependability-related research, in particular computer and network security. Among them are Cambridge University, University of Aberdeen, University of Southampton, Royal Holloway College, University of Strathclyde and Glamorgan University. The University of Newcastle has completed extensive work on risks and issues relating to safety and security risks across interrelated dependent computer networks. In addition, this institution has also been at the core of “dependability related” research activities for over 30 years. These activities have been carried out in continuous cooperation with other leading European and US research and academic institutions. Similarly the Centre for Software Reliability at City University has research capabilities in safety critical software and reliability modelling in software engineering. It is also important to emphasise that this research centre has also started to capitalise on this academic expertise by establishing an advanced in-house safety consultancy house that has carried out software safety assessments for public and private institutions around the world. Finally, academic leadership at City University is looking into integrating safety and security related topics in its many business executive education programmes.

Research into the social and economic implications of dependability take places in a number of domains and think tanks, such as Foundation for Information Policy Research (FIPR), STATEWATCH, Privacy International and the Computer Security Research Centre based at the London School of Economics.

In the area of applied research, a number of important multinational companies have research facilities in the UK. Most relevant are Microsoft, which has its global security research centre at Cambridge, Hewlett Packard with a lab site in Bristol which has extensive capability in cryptography and secure systems design, British Telecommunications has a large research capability in network security, telecom security and intrusion detection at Martlesham Labs. Finally MessageLabs, a global multinational anti-virus company headquartered in London, has pioneered the use of heuristic scanning techniques to predict computer virus outbreaks.