SAINT

Information Assurance: A review of UK Government and industry initiatives

Written by

Nick Coleman

Chair of the Security Alliance for Internet and New Technologies (SAINT)

CabinetOffice

csia
Central Sponsor for Information Assurance

Information Assurance: A review of UK Government and industry initiatives

Written by Nick Coleman,

Chair of the Security Alliance for Internet and New Technologies (SAINT)

Published by the Cabinet Office

CONTENTS

Foreword

Information systems play an essential role in the work of both government and business. In today's 'information society' there is no longer a clear divide between systems in the public and private sectors; they depend on each other to run smoothly and effectively. This means that government must do what it can to ensure the robustness and resilience of information systems to protect the nation's interests. Information assurance is growing in importance. Managing the risks to our information infrastructure is vital and must be built into the core processes of government and business alike.

This report documents the development of information assurance in the UK and its importance to government and to industry. It shows the valuable contribution that many organisations are making in this field. Capturing the range of this work, identifying good practice and understanding the synergies between organisations are extremely important.

A framework has been specifically developed for this report to describe this work. Uniquely, it maps the activities to provide information assurance taking place in the public and private sectors in the UK over the next 18 months. This is the first time that these activities have been identified. The framework provides a model for measuring information assurance and for making international comparisons.

I thank Nick Coleman for his time and assistance in producing this report. I also thank all the organisations mentioned within it that have contributed to its development. I believe that its true strength lies not only in the identification of strong existing relationships across all sectors but, more significantly, in highlighting potential gaps and weaknesses in provision.

I look forward to seeing the plans for future work to secure our information infrastructure that result from this report. It offers an excellent opportunity to continue to develop relationships and cooperation between organisations and with government in this area. This will further the work to achieve full information assurance across both sectors.

Sir David Omand GCB
Security and Intelligence Coordinator and Permanent Secretary, Cabinet Office

Introduction

I am delighted to have authored this first ever review of information assurance in the UK. Information assurance is ensuring that data vital to the functioning of our nation is protected securely. At a time when attacks against our electronic infrastructure continue to grow both in number and levels of sophistication, it is a topic of growing importance.

This review shows the range and nature of work taking place in the private and public sectors to help to protect our information systems. It shares many examples of good practice and innovation that have helped to develop and set ever higher standards of information assurance in the UK.

Although much is being done, there is still more to do. The increased threats facing the UK are such that areas like secure methods for information sharing between the public and private sectors will be an increasing issue going forward.

These issues will also become of increasing importance to the general public. They too need to be made aware of information assurance issues, so that it is not only business people who have the education and are aware about vulnerabilities and the precaution measures necessary.

It goes without saying this report would not have been possible were it not for many industry and government colleagues. I thank all of them for their support.

I also thank Intellect, in particular, Campaign Operations Manager, Ben Brierley, for their help in preparing this report.

Finally, I wish to thank IBM, for their support in giving me the time to write this report.

To take this work forward, I have agreed with Government to assist them in discussing and agreeing the next steps that may be required to address some of the issues raised.

I look forward to working with both industry and government colleagues as we do this and further develop our information assurance capabilities.

Nick Coleman
Chair, SAINT (Security Alliance for Internet and New Technologies)

October 2004

Background

The Central Sponsor for Information Assurance (CSIA) was set up within the Cabinet Office in 2003 to provide a strategic direction for information assurance across the UK. It works with partners in the public and private sectors, as well as with international counterparts, to help achieve a secure and resilient national information infrastructure.

The CSIA aims to assure government that the risks to the information systems that underpin key public interests are appropriately managed.

CSIA defines Information assurance (IA) as the confidence that information systems will:

- protect the information they handle;
- function as they need to, when they need to; and
- be under the control of legitimate users.

The CSIA has a role in pulling together the work to provide information assurance across government, looking at any gaps and overlaps that might need to be addressed. As part of this work the CSIA has identified the need to gain an overview of information assurance across the UK.

Nick Coleman, chair of SAINT, the Security Alliance for Internet and New Technologies, was commissioned to develop a project that would look at the initiatives, strategies and policies that support the protection of information systems, identifying the work being done by organisations in both the public and private sectors. This report is the final stage of that work.

Stage one of this project set out to capture the characteristics of the organisations and the information assurance that they provide.

SAINT approached eight leading organisations providing information assurance activities asking each to describe the:

- aims and make up of the membership of the organisation;
- area(s) and type(s) of information assurance activity that it does; and
- projects and initiatives that it will carry out in the next 18 months.

This information was presented to the Cabinet Office, and an interim report published, in October 2003.

Stage two was to use these findings to devise a framework for understanding the activities.

The framework organised the activities into two groupings:

- categories of activity; and
- themes of activity.

The categories of activity describe the purpose or product of the work. There are five categories:

- web sites;
- guidance;
- meetings/workshops;
- White Papers and reports; and
- research and surveys.

The themes of activity are the areas of information assurance that the work addresses. They are:

- government and industry partnerships;
- governance;
- regulation and certification;
- professional standards;
- business continuity;
- e-crime;
- warning, advisories and reporting;
- security technology best practice;
- security architecture;
- privacy and data protection;
- biometrics; and
- digital certificates and PKI.

For the purposes of this report, the term 'work' encompasses initiatives, strategies, programmes, events, consultations, research, projects, schemes, including actions and activities by the groups mentioned in this report.

This final stage of the project uses the framework to capture the activities of organisations providing information assurance in the UK. The aim is to map the initiatives taking place now and during the next 18 months to see where activity is ongoing and highlight areas requiring additional activity.

To make the project manageable, the report only looks at information assurance activities taking place in or being led from the UK. It does not include activities that have a commercial purpose; this is because including them may contribute to marketing the activity, which is not within the remit of the project.

In order to determine suitable groups, SAINT engaged security leaders and professionals from government and industry to identify organisations to contact.

This was done in three rounds to ensure that the framework provides as reliable and reflective a 'snapshot' of activity as possible.

The following sections of the report summarise these activities.

Table 1. Information assurance initiatives taking place in the public (government) sector:

Themes	Activities				
	Web sites	**Guides**	**Meetings/ workshops**	**White papers/ reports**	**Research and surveys**
Government/ Industry Partnership	CESG NISCC – Information Exchanges and WARPs DTI	NISCC – threat advice CSIA	CESG NISCC – conferences and workshops CSIA	CSIA	NISCC – threat advice DTI – breaches survey
Governance		CSIA	CSIA		
Regulation and certification	CESG Signatures page on DTI web site			DTI – consultation documents on digital signatures	CESG
Professional standards	CESG		CSIA	CESG	
Business continuity	Cabinet Office DTI	DTI promotional material MoD	DTI promotional material CSIA	CESG	CESG DTI – breaches survey
e-Crime	Home Office NHTCU	DTI promotional material Home Office	DTI promotional material Home Office	Home Office NHTCU	
Warnings, advisories and reporting	NISCC – UNIRAS CSIA MoD – JSyCC	NISCC – regular alerts and warnings	NISCC MoD – JSyCC	NISCC	
Security technologies best practice	DTI CSIA	NISCC – guidance and technical notes DTI – security publications MoD	DTI – security publications CSIA ISO/IEC 1779 UK Users Group	CESG CSIA	CESG
Security architecture	CSIA	NISCC – assurance reports	DTI/CSIA participation in Jericho Forum	CESG CSIA	CESG
Privacy and data protection	DCA	DCA		CESG Cabinet Office DCA MoD	CESG
Biometrics			DTI – Innovation Group work with industry groups	CESG	CESG
Digital certificates and PKI	CESG		DTI – EU meetings on e-signatures legislation CSIA	CESG	CESG DTI – further tScheme research

Table 2. Information assurance initiatives taking place in the private (industry) sector:

Themes	Activities				
	Web sites	**Guides**	**Meetings/ workshops**	**White papers/ reports**	**Research and surveys**
Government/ Industry Partnership	SAINT IAAC		SAINT CBI EURIM	SAINT	DTI/PWC[1]
Governance	IAAC	CBI	IAAC CBI i4		ISF survey
Regulation and certification	tScheme	tScheme	tScheme ISO/IEC 17799 UK Users Group IEE	EURIM	
Professional standards	BCS SAINT		BCS SAINT EURIM IEE		
Business continuity		RSMF	RSMF		ISF
e-Crime	APACS	APACS	CBI EURIM BCS RSMF	EURIM	EURIM/IPPR[2] BCC
Warnings, advisories and reporting	WARPs	WARPs	i4 CERTs		NCC
Security technologies best practice	BCC BCS APACS	BCS ISF NCC	APACS BCS BCC i4 ISF ISO/IEC UK	ISF	NCC
Security architecture	ISF BCS i4	NCC ISF	Jericho Group i4		
Privacy and data protection		BCS	EURIM BCS		
Biometrics	IBF	IBF	BCS IBF		IBF
Digital certificates and PKI	tScheme BCC	tScheme	tScheme BCC		

[1] PWC (PricewaterhouseCoopers)

[2] IPPR (Institute of Public Policy Research)

Key findings

There are a number of themes that emerge from the findings. They are outlined in this section.

General

A significant amount of activity to provide information assurance is taking place in the UK. There are more than 30 groups carrying out such work.

The groups vary considerably in the ways that they work and the type of work that they do.

On the whole, the groups are made up from members who choose to join. Typically, members are individuals or organisations responsible for providing information security, either from a vendor or end user perspective.

Activities range from formal work to define common standards for information assurance to informal discussion to help group members share information and best practice.

Target audiences – who these activities are for

Most of the activity is focused at the corporate and public sectors. The number of initiatives aimed at small businesses and home users is currently very low.

Initiatives tend to concentrate on the corporate/public sector information systems in order to:

- specify and set standards for or to improve information security; and
- support or improve the skills and knowledge of the IT professionals and managers responsible for information security.

Some of the newer initiatives are beginning to address the governance issues related to information assurance. These schemes aim to meet the skills needs of individuals with governance responsibilities.

Features of the activities and developing internationality

Few groups attempt to address all areas of information assurance. Most have developed a particular focus of activity, such as trust certificates or corporate governance. As a result, most have a clear focus and are able to take forward specific work.

Several groups are looking at developing international programmes. However, at present most of the initiatives are national in focus.

Developing international programmes and cooperation may provide significant value going forward for these initiatives in areas such as researching the level of security breaches and the development of professional standards.

Involvement in international activity may also indicate that a group will be better able to sustain or develop their work.

Intelligence sharing

Many of the groups and/or their initiatives offer valuable networking and discussion opportunities. In particular, they enable members to give practical help and advice to each other that produce tangible benefits in the services that they provide to their organisations.

However, there are limited models for intelligence sharing between:

- organisations in the private sector; and
- public and private sector organisations.

Where information and intelligence is exchanged, it tends to be between two or more individuals who have built up a trusted relationship.

A number of government-led initiatives are encouraging the exchange of information between public and private sector organisations, as well as between organisations in the private sector. These initiatives focus on e-crime/criminal investigation and information security vulnerabilities.

Models of funding

Several of the groups exist on a restricted amount of funding. The funding is mostly provided by government or by membership fees.

Developing activity

Nearly all industry groups believe that cooperating with other groups will help to increase the effectiveness of their activities and are open to establishing such cooperation.

One challenge to fostering cooperation is that the groups have little knowledge of the work and activities of other groups.

There is some limited communication between industry groups. This is often initiated by an individual or organisation that is a member of more than one group.

The groups contacted for this report feel that the framework will help to support increased cooperation between groups, particularly if the framework is regularly updated.

Taking the findings forward

The Cabinet Office has agreed to hold a review meeting to facilitate the discussion and dissemination of the frameworks of activities and the issues raised by this report.

All of the contributors to this report, along with representatives from the leading vendors, will be invited to attend.

The purpose of the review is to promote discussion on the areas of information assurance across the UK that may benefit from further activity or by being linked together.

In order to support the work of European and other international organisations/groups providing information assurance, the Cabinet Office has agreed that it will assist other national governments, where appropriate, to:

- help them to benefit from the mapping of UK activities;
- develop work to map activities in their countries; and
- develop work that will enable the international mapping and comparison of activities.

Nick Coleman has agreed to support the Cabinet Office and will help international partners understand the details of the report and the key findings, as well as assist other nations in taking similar work forward, if required.

Public sector: central government departments and their agencies

This section provides more information about public sector groups and their activities, in particular, groups led by central government departments and agencies. It was obtained in partnership with the Cabinet Office.

The groups are listed alphabetically.

Cabinet Office, Central Sponsor for Information Assurance (CSIA) http://www.cabinetoffice.gov.uk/csia

The CSIA is a unit within the Cabinet Office that provides a strategic direction for Information Assurance throughout the UK. The CSIA works with partners across government and in the private sector, as well as its international counterparts to help maintain a reliable, secure and resilient national information infrastructure.

The CSIA has produced a UK Government National Strategy for Information Assurance for the Cabinet Office Committee on Security (SO). The aim of the strategy is to ensure that the risks to the key systems underpinning public interests are managed appropriately.

The strategy recognises that in order to protect the UK information infrastructure, it is necessary to promote information assurance best practice across both the public and private sectors, as well as to home users of information systems.

The CSIA responsibilities are to:

- provide a strategic direction for information assurance across the whole of the UK;
- coordinate and complement the activities of parties contributing to information assurance;
- sponsor 'common good' activities that benefit the development of information assurance;
- accredit pan-government systems and in some cases, such as the Government Secure Intranet (GSI), own and manage the risk to shared information; and
- promote and support the resilience of IT and telecommunications infrastructures.

Activities and ongoing work

Over the next 18 months the CSIA will deliver work in the following areas:

Outreach:

- To promote IA best practice across all sectors, in particular, the CSIA will work with other government departments and industry to promote Internet security awareness to the general public and micro-organisations;

IA products and services

- General IA Products and Services Initiative (GIPSI) will produce a risk assessment/management approach to define security processes and requirements for secure products and services. Within the work of GIPSI, the CCTM (CSIA Claims Test Mark), aims to provide a basic level of assurance to a range of IA products and services for use in the public and private sectors, as well as by home users. A pilot will begin in early 2005;

- CIPCOG is a collaboration between the OGC, CESG and CSIA and provides a forum for facilitating the development and deployment of IA products and services that meet the business requirements of the wider public sector.

Governance:

- Sir Andrew Turnbull, the Cabinet Secretary, established the management of information risk as a key board level function in departments and he requested that a board member is designated as the Senior Information Risk Owner (SIRO). The cross governmental network of SIROs is working through the CSIA and its partner organisations to help measure and improve information risk governance allowing potential business benefits of ICT to be realised.

Public/private sector partnerships:

- work with information assurance organisations, including IAAC, SAINT and Foresight, to promote best practice to all sectors;

Training and professionalisation:

- address training and standards for professionals in the field of information assurance, in conjunction with other government departments and private sector organisations;

- produce a database of organisations that provide training for information assurance professionals in the public sectors;

- analyse training needs and the availability of courses; and

- research the feasibility of defining standards for information assurance professionals.

Communications–Electronics Security Group (CESG)
http://www.cesg.gov.uk

CESG is the Government's National Technical Authority for information assurance. It is responsible for enabling secure and trusted knowledge sharing to help central government departments and agencies, the Armed Forces and law enforcement authorities to achieve their corporate objectives.

CESG is a part of Government Communications Headquarters (GCHQ).

Activities and ongoing work

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. To do this CESG provides information assurance policies, services and advice to government and other customers. This includes:

Technical advice:

- initial technical advice on design options for secure IT architectures;
- in-depth technical consultancy on specific information assurance issues;
- help with interpreting national security standards such as BS 7799;
- guidance on the use and deployment of cryptographic and other certified information assurance products; and
- advice on algorithm use and suitability.

Documentation:

- production of system security documentation, such as system security policy (SSP) and security operations procedures (SyOPs);
- advice on sources and status of technical documentation; and
- verbal and written feedback on technical documentation.

Other services include providing:

- continuity of information assurance advice throughout the life of projects;
- information on suppliers of approved and certified products;
- help-desk style telephone advice;
- access to alternative sources of technical advice; and
- training on specific information assurance issues.

As part of Government's drive to improve the culture of security throughout the public sector, CESG is working as part of a team that is looking at making policy and guidance documentation more widely available. Much of the existing documentation is neither relevant to, nor written in appropriate language for, the wider public sector. The aim of this work is to understand the information assurance needs of the wider public sector and to tailor existing policy and guidance documents to this community.

Department for Constitutional Affairs (DCA)
http://www.dca.gov.uk

The Department for Constitutional Affairs (DCA) is responsible in government for upholding justice, rights and democracy. Its aims include safeguarding the rights of citizens.

The Information Rights Division within the DCA has responsibility for policy on freedom of information and data protection, and general data sharing issues.

Activities and ongoing work

In November 2003, DCA guidance was produced setting out the legal framework that applies to data sharing. In particular, the framework set out the use of personal data, across traditional boundaries, by the public sector to achieve better policies and deliver better services for individuals and society as a whole.

A tool kit on data sharing for the pubic sector has been developed and is available on the DCA web site. It includes guidance and examples of good practice on information handling, such as data protocols. The DCA will regularly add to the tool kit, until it contains a complete set of guidance on data sharing. A key part of the tool kit is the addition of the 'Public Sector Guarantee'.

Extensive consultation and discussion with key stakeholders has taken place to produce the Public Sector Guarantee, which will be launched on the DCA web site soon. The purpose of the Public Sector Guarantee is to reassure people that safeguards are in place when they supply personal information to the pubic sector. Its use in the public sector is voluntary. However, all central government departments will use it.

Work is underway to look at how best the DCA can work with partner organisations and stakeholders to provide training, education and support to front line staff dealing with sharing of data issues.

Department of Trade and Industry
http://www.dti.gov.uk

The Department of Trade and Industry (DTI) works with businesses, employees and consumers to drive up UK productivity and competitiveness by enabling and encouraging confidence in the use of new information and communications technologies.

It has responsibility for all businesses, including SMEs (small and medium sized enterprises) and customers in the critical national infrastructure. The Department is committed to promoting good information security practice as part of its efforts to make the UK the best place for e-business.

Activities

The DTI works with business to raise awareness of the importance of effective information security management and to encourage the adoption of security standards, such as ISO/IEC 17799 and BS 7799.

In partnership with industry, it produces biennial information security breaches surveys. The most recent survey, produced with PricewaterhouseCoopers, was published in April 2004. The surveys are intended to help businesses understand the information security risks they face. They also help inform the DTI's own activities.

The findings of previous breaches surveys showed that smaller companies found it difficult to obtain easy-to-understand infosec (information security) guidance. To respond to this, the DTI has set up a web site and developed a suite of supporting material to encourage and support best practice in this area. The focus is on security as a business enabler. The web site offers easy-to-understand help and guidance for all companies, but particularly for SMEs.

The DTI is involved in various initiatives to promote the use of ISO/IEC 17799 and BS 7799 – the international and British standards on information security. It runs a UK Users' Group for the standards that includes some 550 large and small companies, as well as central government departments and local authorities. Members are either using the standards or are interested in doing so. The DTI produces regular newsletters for members and organises several workshops each year. The group is managed by an industry steering committee.

The DTI is also involved in the organisation of the international '7799 Goes Global' conferences. Take up of the standards in the UK and overseas has increased significantly during 2004. These standards help organisations to implement best practice in information security management and provide specified levels of assurance for suppliers and customers.

Providing a policy framework to encourage improved information security, both at home and internationally, is another area of activity.

In 2002, the DTI helped to produce the OECD (Organisation for Economic Cooperation and Development) *Guidelines for the security of information systems and networks: Towards a culture of security.*

The DTI plays a leading role in the European Network and Information Security Agency (ENISA), which was launched in March 2004. This new agency will support the achievement of high levels of network and information security within the European Union. The aim is for ENISA to become a centre of excellence, providing advice to Member States on network and information security issues. Business will have input into the direction of the agency and will benefit from the work to reduce vulnerabilities and increase the understanding of information risk.

The DTI continues to provide support industry-led initiatives, such as SAINT and tScheme.

Ongoing work

DTI will progress these activities. In particular, it will continue to develop the guidance materials for SMEs and focus on outreach work.

Several projects are being developed with various business organisations to increase awareness of good information security practice.

Home Office
http://www.homeoffice.gov.uk

The Home Office's responsibilities cover crime, policing, criminal law and counter-terrorism, as well as immigration control, prisons, probation and promoting active citizenship and cohesive communities.

The Home Office also has responsibility for criminal law in England and Wales, including the Computer Misuse Act, ensuring that criminal law keeps up with new ways technology provides for committing offences and negotiating international treaties, such as the Council of Europe Cybercrime Convention and the EU Framework Decision on Attacks Against Information Systems.

The Home Office has policy responsibility for the balance between law enforcement agencies need to get intelligence and evidence about individuals and protecting individuals' privacies and freedoms.

Activities and ongoing work

The Home Office sponsors police forces in England and Wales, as well as the new Serious Organised Crime Agency, which will effectively amalgamate National Crime Squad (including the National Hi-Tech Crime Unit (NHTCU), National Criminal Intelligence Service, the part of HM Customs and Excise that deals with drug smuggling and the part of the Home Office that deals with organised immigration crime, by 2006.

A programme of work is ongoing to ensure the new Agency and the police are well placed to deal with computer crime in the future.

Computer crime presents new variations on the challenge of traditional crime to law enforcement. The global nature of the Internet also emphasises the need for effective and timely international cooperation.

The Government e-crime strategy to be published later this year, aims to provide a coherent, consolidated statement of the Government position across departments in relation to e-crime. It will provide a framework for Government, law enforcement and industry action in response to e-crime, seeking to resolve specific questions and to focus debate on longer term issues.

The strategy will focus on a number of issues, including the e-crime information base, reporting of e-crime, crime reduction and prevention, legislation, the policing response and the role of business and community in combating e-crime.

The Home Office Crime Reduction and Community Safety Group (CRCSG) aims 'to reduce organised and international crime and to combat terrorism'. Within CRCSG, the Terrorism and Protection Unit (Protective Security) has the lead policy role for ensuring that the UK's Critical National Infrastructure is protected from electronic attack. The Terrorism and Protection Unit, therefore, works closely with and as part of the National Infrastructure Security Coordination Centre (NISCC).

The Organised and Financial Crime Unit (OFCU), which is also part of CRCSG, has the policy lead on tackling organised crime in England and Wales, including the development of the national e-crime strategy. The OFCU funds and works very closely with the NHTCU.

The Fraud Team in the OFCU works with business to reduce business crime and encourage crime resistant products. The Fraud team has responsibilities that relate to the reduction of credit card fraud. It works with the DTI, Department for Culture Media and Sport and the Patent Office on combating counterfeiting and piracy.

The Identity Cards Programme Team in the Home Office is engaged in work on personal identity issues and trust in relation to the information society and the development of entitlement cards.

Outreach to industry takes place through various initiatives, for example, the NHTCU Outreach Programme and Confidentiality Charter. The NHTCU outreach programme seeks to advise businesses on crime reduction measures, the need to report incidents and also highlights the need for firewalls and anti-virus software. Other industry outreach initiatives are promoted at local level by individual forces.

There is also the Internet Crime Forum, a joint industry, government and law enforcement group which works to promote, maintain and enhance effective working relationships to tackle crime and foster business and public confidence in the use of the Internet.

The Home Office's work includes discussion with the European Union and Member States, the G8 countries and participation in various other international fora, including the G5, Council of Europe and UN, as well as bilateral contact with international colleagues.

Information Commissioner's Office (ICO)
http://www.informationcommissioner.gov.uk

The Information Commissioner is an independent authority, appointed by the Queen, who reports annually to Parliament. The Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000, which both relate to the handling of information.

The current Commissioner is Richard Thomas.

Among other obligations, the Data Protection Act 1998 (DPA) requires that public and private sector organisations have appropriate technical and organisational measures in place to ensure that information is kept secure against unauthorised or unlawful processing and accidental loss or destruction of, or damage to 'personal data'.

Personal data is information identifying individuals, which is processed automatically and in some manual filing systems.

The Freedom of Information Act 2000 (FOIA) provides individuals with a right of access to information held by pubic bodies and designated private sector organisations. Under Section 46 of the Act the Lord Chancellor may issue a code of practice providing guidance to relevant authorities subject to the Act about good practice in the keeping, management and destruction of their records. The Commissioner promotes the following of good practice and, in particular, observance with any code of practice issued under Section 46 of the Act.

Activities and ongoing work

The Commissioner has a duty to promote good practice in information handling and responds to Government consultations and initiatives to ensure that the legal requirements of the legislation that he oversees are considered.

The Commissioner also provides guidance in response to specific requests and in the form of good practice notes and codes of practice, where a wider need is perceived. Among the objectives in the Information Commissioner's Office corporate plan for 2004/07 is a commitment to ensure the provision of timely and simple guidance to organisations to enable them to comply with the DPA and FOIA.

At the request of individuals whose information is being processed, the Commissioner assesses compliance with the DPA. In 2003/04 the Information Commissioner's Office made approximately 4,700 assessments and expects to make a similar number in 2004/05. The Commissioner can take action to enforce compliance with the Act where such an approach is appropriate and necessary.

The Commissioner conducts audits of organisations' compliance with the DPA when invited to do so by the organisation. The Commissioner has also produced an audit manual that organisations can follow if they choose to conduct such audits themselves.

From January 2005, if it appears to the Commissioner that relevant bodies subject to the FOIA are not conforming to the standards recommended in a code of practice under the same Act, he may issue a practice recommendation, in cooperation with the National Archives, with whom the Information Commissioner has signed a memorandum of understanding.

Ministry of Defence
http://www.mod.uk

The Ministry of Defence (MoD) has a responsibility for promoting security including promoting the implementation of information assurance. The MoD works closely with the Foreign and Commonwealth Office (FCO), Home Office, DTI, Cabinet Office and their agencies to achieve this.

It has 300,000 civilian and Armed Forces personnel using at least 160,000 workstations on scores of LANs (local area networks).

Activities and ongoing work

In 2003, the MoD achieved BS 7799 for the security management of its information systems. This work included restructuring the main MoD security policy document to align it with the structure of the Cabinet Office Manual of Protective Security. MoD also ensured that the BS 7799 controls were encapsulated in the security policy document or in other information management publications.

Over the next 18 months, MoD will carry out work to:

- complete the implementation of the Security Awareness For Everyone (SAFE) Campaign. This programme has been designed to raise a general awareness of information assurance across the defence community. This is initially being achieved by giving presentations at various in-house conferences, security related articles in in-house publications and the use of low cost, high volume promotional items, such as pens and coasters, each bearing a security message;
- launch a new in-house magazine, *ITSO FACTO*, specifically aimed at information assurance security officers. Among other topics, it will carry articles on specific information assurance issues, useful tips and guidelines and answer FAQs. This should provide security officers with information to help make their individual sections more secure;
- develop policy to address emerging threats from mobile devices. It will include comprehensive advice on USB (universal serial bus) memory devices, mobile phones, cameras, Bluetooth, and so on;
- review all information security policy documents to meet the requirements of the Freedom of Information Act (2000);
- expand the Joint Security Coordination Centre (JSyCC) to provide comprehensive CERT services to the MoD as a whole;
- re-launch a web site on the MoD Intranet that will answer staff queries about information assurance; and
- develop a new policy document to provide guidelines for Computer Network Defence (CND) Alerts and Warning and Response procedures for MoD.

In conjunction with the Communications–Electronics Security Group (CESG) and a number of other government departments, the MoD is involved in the revision of HMG (Her Majesty's Government) Infosec Standard No 2, which covers risk management and accreditation of information systems.

National Hi-Tech Crime Unit
http://www.nhtcu.org

The National Hi-Tech Crime Unit (NHTCU) is a national law enforcement unit that combats hi-tech crime in, or which impacts, the UK. It was set up in 2001 as part of the national hi-tech crime strategy. It aims, through sustained leadership to define, demonstrate and discharge world class standards in combating hi-tech crime. Since it was created, computer crime units have been set up in local police forces and a national centre for excellence has been established.

The NHTCU is a multi-agency unit, accountable to the Director General of the National Crime Squad and to the National Crime Squad Service Authority. It draws skilled and experienced staff from National Crime Squad (NCS), the National Criminal Intelligence Service (NCIS) and Her Majesty's Customs and Excise (HMC&E). It works in partnership with other agencies to prevent and detect serious and organised computer-related crime.

The strategic direction of the NHTCU is set by the Strategic Stakeholders Group (SSG), which also champions the hi-tech crime strategy.

The SSG is made up of representatives from UK law enforcement agencies, the Crown Prosecution Service (CPS) and a representative from industry.

Hi-tech crime, also known as 'cybercrime', encompasses a variety of computer-supported criminal activities, including fraud, hacking, virus and denial of service attacks, software piracy, online child abuse, fraud and identity theft.

Activities and ongoing work

Activity focuses on emerging technologies and how they may be used to commit serious and organised crime. However, because these technologies are widely available, use of them to commit crime is also part of general law enforcement. In particular, NHTCU has worked closely with the private sector to police cyberspace and establish an e-marketplace protected from 'lawlessness'.

The Confidentiality Charter, which was launched in December 2002, is designed to help business understand how it can interact with the NHTCU in a secure, efficient and confidential manner to exchange information, report hi-tech crime and seek advice. The requirements of the Charter came from the NHTCU's Outreach Programme. This is a strategy to enable business and the NHTCU to communicate more effectively with each other and to help business understand how law enforcement works. It has produced a significant increase in cross-sector intelligence flows with mutual benefit.

In 2004, NHTCU commissioned and published its second survey of the effect of hi-tech crime on businesses. The work was carried out by market research company NOP, with assistance from Nick Coleman at SAINT. It supports other work to provide a better understanding of business issues in relation to computer-related crime.

The study examined the impact of hi-tech criminality on 201 UK-based companies and how those companies perceived the ability of law enforcement agencies to tackle incidents.

It was launched at NHTCU's e-Crime Congress event. The e-Crime Congress is also a part of the outreach strategy. This conference brings the business community and law enforcement agencies together to build trust, increase dialogue and encourage the reporting of e-crime. The 2004 e-crime congress attracted over 400 delegates from industry and law enforcement. The NHTCU is currently planning the 2005 e-crime congress.

National Infrastructure Security Coordination Centre (NISCC)
http://www.niscc.gov.uk

NISCC was formed in 1999 and draws on the expertise of a range of UK government departments. Key players are the Cabinet Office, CESG, the Security Service (MI5), National Hi-Tech Crime Unit, (NHTCU), Defence Science and Technology Laboratory, Ministry of Defence (MoD) and Department of Trade and Industry (DTI).

NISCC is led by a director and is accountable to the Home Secretary.

Activities

NISCC works to minimise the risk of electronic attack (eA) against the UKs critical national infrastructure (CNI).

The CNI are the crucial systems run by government and the private sector that support everyday life, this includes the vital computer services that underpin them. These crucial systems cover ten sectors: communications, emergency services, energy, finance, food, government and public services, public safety, health, transport and water.

Failures in one sector can seriously affect another and the increasing dependence on the Internet means many of these systems are vulnerable to attack.

NISCC is responsible for implementing a programme for protecting the CNI from interference and disruption. Its main duties are:

- issuing technical alerts and warnings;
- offering protective security advice;
- fostering best practice;
- encouraging and facilitating information sharing;
- investigating and assessing threats;
- conducting research and development work; and
- developing strong international partnerships.

Ongoing work

Over the next 18 months NISCC plans to:

- expand the number of Information Exchanges – public and private sector partnerships which facilitate the flow of confidential and sensitive information within the CNI – across a wider range of sectors and technologies;
- enhance and extend its vulnerability disclosure process to make the CNI even more resilient;
- undertake research, with a range of partners, to continue the process of identifying potential vulnerabilities and other weaknesses and ensure speedy remediation;
- continue to support and promote effective response and best practice by issuing timely warnings, threat advice, practical guidance and good practice materials;
- encourage the spread of Warning, Advice and Reporting Points (WARPs) across the UK;
- expand work with companies at the heart of the CNI to assure the level of protection of their systems, give focused advice on the threat, awareness of attack and possible improvements to their risk management processes; and
- improve communications, sharing and understanding with international partners and define Critical Infrastructure Information Protection protocols on a global basis, through partner agreements with colleagues in North America, Europe and South East Asia.

Private sector: industry groups and activities

Summary of activities

There is a wide range of work underway in the private sector.

The groups are listed in alphabetical order.

APACS (Association for Payment Clearing Services) http://www.apacs.org.uk

APACS (Association for Payment Clearing Services) is the UK payments association, a trade association of institutions delivering payment services to end customers. It provides the forum to address cooperative aspects of payment services and other payment-related developments.

APACS focuses on payment services provided to UK customers – both domestic and cross-border payments. However, the context is increasingly European, and to a lesser extent global, because this is the regulatory and market scope.

These services include all payment types – cash, card payments, automated credit transfers, direct debits, cheques and emerging payment methods.

APACS activities potentially cover all parts of the end-to-end payment process, in particular, with respect to its 'integrity' and 'standards' roles. The appropriate cooperative/competitive boundary is agreed for each activity.

Payment-related areas such as fraud control, card credit risk management and liquidity management are also covered where these impinge on payments.

APACS' core roles and objectives are:

Vision and strategy:

- to define, articulate and promote a vision and strategy for the UK payments industry, in the context of domestic, European and international developments to ensure that end customer requirements can be delivered in an economically sustainable manner;

External communications:

- to be the respected spokesperson for the payments industry and an authoritative source of payment knowledge; and
- promote the understanding of payments and payment-related issues to interested stakeholders and the general public, in order to secure public confidence in, and improve public perception of, the payments industry;

Change management:

- to support and encourage the development of existing payment services and the establishment of new payment services to better meet member and stakeholder requirements;

Integrity:

- to protect and enhance the integrity of the payments industry and to promote world-class management of payment system risks. This includes risk management, fraud management, pan-scheme settlement risk, security and business continuity; and

- to facilitate and promote the development of industry measures to reduce payment-related fraud and criminal activities in payments;

Standards and interoperability:

- to develop and promote world-class standards for use in UK payment services in the context of European and international developments.

Activities and ongoing work

The APACS core role of 'integrity' relies on a wide range of information assurance and technical information security activities. These are all designed to support the goal of ensuring trust and confidence in the payments services the members supply. This includes work to:

- develop security standards for banking and information protection in payment schemes;

- provide separate products to address security issues in individual payment schemes; and

- manage collaborative sub-groups that deal with specific payment services.

Key APACS projects include the:

- 'Chip and PIN' programme, which is being introduced to increase the security of card transactions. Chip and PIN is large-scale joint project between the UK retail and banking industries. The programme is aimed at the general public, as well as individuals and organisations with responsibility for providing information assurance. APACS will contribute to a range of events publicise and roll out this programme;

- combating of card fraud by developing education and public awareness programmes for consumers and retailers. APACS also provides the Card Watch web site. Card Watch is a UK banking industry body that works with the police, retailers and other organisations to tackle card fraud;

- development of material to inform the wider public of the dangers of identity fraud, and training material and products to support business in detecting such fraud; and

- support of members with the detection and coordination of incident response to attacks against e-banking customers through 'phishing' and malicious code designed to record online banking activities. This includes the development of media and consumer awareness material to help consumers bank safely online;

British Chambers of Commerce
http://www.chamberonline.co.uk

The British Chambers of Commerce (BCC) aims to help UK businesses succeed and grow. It is a not-for-profit, national network of accredited Chambers of Commerce representing thousands of businesses in the UK.

BCC see its stakeholders as being its UK business members and partners with a special interest, including Trustis, Microsoft, British Telecom, DTI, Hewlett Packard, Intel and Royal Bank of Scotland. Its messages are targeted to the UK business sector and influential figures in Government and the public sector.

Activities

BCC is involved in a number of initiatives that aim to help business understand the benefits of using the Internet and providing a secure environment for e-business. This work includes developing authentication and trust services. BCC has set up a web site to explain these services.

Ongoing work

BCC has developed a portfolio of digital certificate based services operating to tScheme guidelines at government security level 2 or 3. Authentication of users is carried out either face-to-face or remotely, depending on the appropriate level of security, before a certificate is issued.

BCC is launching an SSL Server Certificate service to support secure e-commerce. The certificates will provide a 'hallmark' of authenticity for a business's web site to show that the provider is known and trusted by other businesses and their customers.

In association with the DTI, BCC runs e-business clubs to promote confidence in the use of the Internet for business. In 2003, BCC organised a programme of UK-wide security seminars, in association with Microsoft, to raise awareness of the importance of IT security to the SME business community.

In April 2004, it published a major survey of crime against business that included information about e-crime.

BCC researches the experiences and opinions of member businesses to develop policy papers.

British Computer Society
http://www.bcs.org.uk

The British Computer Society (BCS) is the industry body for IT professionals and a Chartered Engineering Institution for Information Technology (IT).

BCS was set up in 1957 and became a chartered engineering institution in 1989. It has more than 38,000 members from countries around the world, including 8,500 chartered engineers.

The society is governed by a Trustee Board that includes five professional members elected by an advisory council. It has a number of boards and committees that are responsible for strategic areas of activity.

Activities

BCS develops and implements standards of education and experience for professionals working in the field of computers and information systems.

It also promotes awareness of the social and economic benefits of IT. This includes increasing understanding of what is required to implement successful IT projects and programmes.

Ongoing work

BCS' activities will be in the areas of governance, privacy and data protection, e-crime, regulation and certification, biometrics and digital certificates/PKI.

Over the next 18 months BCS plans to:

- establish relations with the Information Commissioner's Office to encourage understanding and acceptance of the requirements of Data Protection Act (DPA);
- work with the National Hi-Tech Crime Unit (NHTCU) and the High Technology Crime Investigation Association (HTCIA) to promote secure business processes and to encourage the reporting of hi-tech crime; and
- promote the Information Systems Examining Board (ISEB) Advanced Diploma in Information Security Management Principles Certification. The BCS provides industry-recognised qualifications in information security through the ISEB that aim to raise industry standards.

BCS is involved in the consultation on the Government proposals to introduce national identity cards, in particular, the biometric technology required to support them.

BCS is also considering the use of PKI and digital certification for its internal information networks.

Confederation of British Industry
http://www.cbi.org.uk

The main objective of the Confederation of British Industry (CBI) is to help create and sustain the economic and social conditions that allow business in the UK to compete and prosper. Through its network of offices around the UK, in Brussels and Washington, it represents its members views on all cross-sectoral issues to government and other national and international policy-makers.

The CBI supplies advice, information and research services to members on key public policy issues affecting business and provides a platform for the exchange and encouragement of best practice.

It lobbies national and regional government and administrative bodies in the Britain, EU and USA on the behalf of UK business.

It was founded in 1965 and is a non-profit making, non-party political organisation, funded by the subscriptions paid by its members.

The CBI has a membership of nearly all of the FTSE100 companies, many trade associations and small and medium sized businesses.

It is structured into sector committees operating in 11 regions across the UK.

Activities and ongoing work

Information Security is dealt with within the e-Business team and is also covered by the Company Affairs Group that looks at data protection issues.

The CBI will respond to Government proposals for legislation, including the Draft Identity Cards Bill and RIPA Part 3. It also plans to respond to the proposed EU Framework Decision on data protection.

The CBI will continue work to build public-private sector dialogue to:

- improve government understanding of business concerns and help shape policy; and
- ensure that businesses are aware of government programmes, such as the e-Crime Strategy, National Hi-Tech Crime Unit information campaigns, as well as EU initiatives, for example, ENISA (European Network Information and Security Agency).

There are a number of initiatives to improve business preparedness for security vulnerabilities. The CBI plans to:

- produce a guide on information security for SMEs focusing on critical electronic business supply chain issues;
- contribute to the development of trust marks, including tScheme, to provide authentication security models; and
- support the CSIA's work on information assurance.

The CBI also plans to re-structure its e-Business Council to enable work to:

- develop greater understanding across the wider e-business community (users, suppliers and content providers) of the importance of implementing information security measures in company policies and practices; and
- identify business processes that promote efficiency across supply chains and information security best practice, in order to build the case for return of business investment.

EURIM (European Information Society Group) http://www.eurim.org

EURIM, the European Information Society Group, is a parliament/industry group that raises concerns about information, communication and technology policy with government.

It is an independent, all-party group based in the UK and funded by its members.

Membership includes Cabinet Ministers, Ministers, MPs, MEPs, Peers, Parliamentary Private Secretaries, committee chairs and presidents, former Ministers and opposition spokespersons. It has 48 corporate members, including blue-chip companies, financial institutions, broadcasters, publications and professional bodies. The 35 associate members include trade associations, professional bodies and smaller not-for-profit organisations.

EURIM achieves its objectives by influencing the law-making processes through high-level political contact and working with those responsible for drafting policy.

Activities and ongoing work

EURIM activities in the area of communications regulation includes work on:

- privacy;
- data protection;
- surveillance;

- skills and learning networks;
- e-commerce transactions and payment;
- socio-economic vulnerabilities after 9/11;
- fair dealing and intellectual property rights;
- parity between online and off line legal obligations; and
- UK/EU competitiveness and the Pacific Rim.

Activities in the area of e-crime includes work to look at:

- the scale and nature of computer-assisted crime;
- the reporting of e-crime;
- roles, procedures and skills for security and investigation;
- reducing vulnerabilities and opportunities; and
- legal issues arising from data sharing – including within the context of law enforcement, and personal identity – including within commercial and international environments, as well as issues to do with identity cards;

EURIM is working with the Institute for Public Policy Research (IPPR) on a study of partnership programmes for policing the information society.

Final reports produced for this study have made recommendations about the scale and nature of computer-assisted crime, reducing vulnerabilities among small firms and the skills needed to do this.

A number of draft reports have also been published. They make recommendations on roles and procedures, 'designing out' opportunities to exploit vulnerabilities in information systems and prevent e-crime, reporting and legal issues to do with e-crime.

The next phase of the study will produce work to:

- reduce vulnerabilities and proactively 'design out' opportunities for e-crime in trading;
- address legal issues following on from the all party Internet inquiry into the Computer Misuse Act 1990; and
- take forward the recommendations that have been agreed.

The Information Assurance Advisory Council
http://www.iaac.org.uk

The Information Assurance Advisory Council (IAAC) aims to advance information assurance to build a robust, secure foundation for the UK's information society. It does this by engaging key public and private sector bodies in the work to create secure information systems.

It is a private sector-led, not-for-profit group. There are more than 70 members from academic institutions, public and private sector bodies, international organisations and individuals.

IAAC is governed by a board with representatives from Microsoft, HP, RAND Europe, Qinetiq, Symantec, Anite Public Sector and Cisco.

It also has a Government Liaison Panel; members include representatives from CESG, the Cabinet Office, NISCC and DTI.

Activity

IAAC focuses on promoting the awareness of information assurance as part of the process of strategic governance, particularly at board level within companies and organisations.

Ongoing work

Current activities include work to:

- support the development of a national strategy on information assurance and cybercrime, and encourage its implementation;
- provide strategic analysis and develop resources that meet the needs of individuals with governance responsibilities, particularly at board level, using the regulatory framework in the US and the EU;
- develop strategies to promote awareness of risks and look at how to address these issues with the general public, as well as with business and regional administrations; and
- identify further capacity needs for those with responsibility for providing information assurance and support the development the products and services that will address those needs.

IAAC also plans work to take forward the Cyber Trust and Crime Prevention project, launched by the Office of Science and Technology Foresight programme. The project explores the application and implications of next generation information technologies.

International Biometric Foundation
http://www.ibfoundation.com

The International Biometric Foundation (IBF) aims to provide a forum for impartial and educative discussion of the use of biometrics and related technologies.

IBF was set up in December 2003 and is a not-for-profit organisation. It brings together government, academic institutions and bodies, industry, media and users from around the world and has over 60 members.

Activities

The IBF works to develop and set standards for the use of biometrics and biometric technologies used to support information assurance. This includes:

- specifying relevant standards or suggesting additional standards where appropriate;
- highlighting and promoting awareness of operational issues that affect the integrity and performance of applications;
- identifying and raising awareness of ‘human factor’ issues that affect correspondence to ‘realised performance’;

- examining related processes of biometric enrolment and how they affect the integrity of operation of a biometric system; and
- evaluating biometric techniques from a practical and operational perspective.

Ongoing work

Current projects include:

- the development of the first version of the Biometric Operability Index. This aims to provide common measurements of the performance of biometric techniques for specification and procurement purposes;
- the production of the first draft of a biometric registration model, which aims to provide a common framework for capturing key attributes when enrolling people into wide scale applications in the public sector to assure confidence when accepting documents or tokens registered by another authority;
- the development of a personal identity XML schema for coding biometric measurements, including programs to support it;
- the development, with the application development tools community, of robust components for the integration of biometrics into host applications in a consistent, reliable and secure manner; and
- the production of a vision for biometrics over the next 25 years, showing IBF's view of the potential development, changes in the technologies and usage.

Continuing work includes:

- further development of teaching and training programmes to promote awareness of the issues to do with wide-scale implementation of biometrics and related technologies; and
- an online survey of the end users of biometric technologies to monitor awareness and understanding from their perspective of associated issues, including trust, data protection and the security of information.

The IBF will also continue to liaise with international groups to discuss biometric issues and provide advice.

Institution of Electrical Engineers
http://www.iee.org

The Institution of Electrical Engineers (IEE) was founded in 1871 and is the largest engineering institution in Europe with a membership of some 130,000 professional engineers. Members represent key sectors of international business and commerce, including communications, computing, electronics, energy, information technology, manufacturing and transport.

It has a global network of over 90 branches worldwide and 1000 business partners. The IEE executive also provides support to 35 professional networks, eight industry sector panels and five policy advisory groups.

The UK Computing Research Committee (UKCRC), a group of the UK's leading computer science researchers, formed to represent and promote the best interests of computing research, is recognised as an advisory panel by the IEE.

Activities

The sectors from which the membership and business partners are drawn are critically dependent on assured information for both business purposes and the automation, control, measurement and monitoring of processes – such as manufacturing, transport movements, healthcare, power and building services, including safety critical systems.

Many of IEEs members and business partners deliver elements of the Critical National Infrastructure (CNI) for which continuity and, therefore, information assurance is vital. Loss, significant interruption or degradation of these services would have life-threatening, serious economic or other grave social consequences.

Ongoing work

The IEE will contribute to information assurance by:

- responding to Government consultations and submissions to Parliamentary committee inquiries on EC and UK legislation and regulation in areas such as data protection, data privacy, data access, digital signatures, electronic commerce, business crime and forensic practitioners. For example, the Computer Misuse Act and the Draft Identity Cards Bill;
- contributing to strategic research to take forward the results of the DTI/Industry Office of Science and Technology Foresight Cyber Trust and Crime Prevention project. IEE will also support other crime science initiatives, including the Engineering and Physical Sciences Research (EPSRC) Crime Prevention Research Programme;
- participating in 'agenda for change' activities, for example the EURIM-IPPR e-crime study;
- supporting policy development and implementation work of best practice with key Parliamentary groups (for example, PITCOM, the Parliamentary Information and Technology Committee), Government departments (for example, Office of Government Commerce), business organisations (for example, BuyIT), and academia (for example, UKERNA – the United Kingdom Networking and Research Association). This includes supporting work to build on and promote best practice that has been developed by others;
- publishing books, journals, magazines and conference materials;
- arranging in learned society and professional institution events, including collaborative activities;
- promoting professionalism throughout the ICT sector and beyond, in particular, through work with e-Skills UK and the Skills Framework for the Information Age Foundation; and
- continuing to develop and publish guidelines about best practice in information security, *The Risk of Computer Crime to Small and Medium-sized Enterprises – What your business really needs to know.*

International Information Integrity Institute (i4)
https://i4online.com

The International Information Integrity Institute (i4) provides a secure environment to allow international businesses to confidentially share ideas and concerns about information security and risk.

It works with its members to:

- explore information-related business risks; and

- help them to develop cost-effective security programmes to support global business.

Confidentiality is established by a mutually-respected formal agreement between members.

i4 was formed by SRI International (formerly Stanford Research Institute) in 1986. It is now managed by the independent information security consultancy, RedSiren.

More than sixty 'Global 1000' companies are members of i4. A number of them have their headquarters in the UK.

Members meet to exchange strategies, ideas, experiences and expertise on managing information-related business risks, with input from selected experts from industry and academia.

A member advisory committee, elected from the membership, approves i4s programme of activities.

Activities

The activities centre on providing the means for members to communicate and collaborate with each other.

i4 Forums are held three times a year where members can network, make formal presentations with follow-on debate and hold informal discussions about leading-edge information risk management and protection.

One-day regional meetings are held a least six times a year. These allow members to explore issues in greater depth than at the forums.

There is a secure web site for members to retrieve information from the repository of meeting records and i4 reports. Members also post queries to the wider membership for advice. Dialogue and analysis of these queries are summarised in a monthly newsletter.

i4 also issues several reports a year about key issues in security technology and management. The reports are developed by RedSiren staff in conjunction with i4 members or are the work of i4 alliance partners.

The group has access to a number of major research centres to develop this programme, including SRI International, CERT® Coordination Center, Carnegie Mellon University, the Internet Security Alliance, Royal Holloway University London and the London School of Economics.

Ongoing work

There is a rolling programme to provide meetings and information resources to members. This work will help members to:

- address risk management, looking at the business value of information assurance;
- identify and describe the capabilities and risks of new technologies;
- support the creation of risk managed environments by developing security architecture and strategies;
- explore the issues of integration and deployment and 'legacy retirement' (the replacement of old information systems and programs with new ones);
- establish proactive and reactive capabilities for responding to vulnerabilities; and
- identify the current and emerging impacts of the regulatory environment.

Information Security Forum
http://www.securityforum.org

The Information Security Forum (ISF) supports the development of information assurance by funding research into information security that it uses to develop best practice guidance for its members.

It is a not-for-profit, international association that was set up in 1989. It has members from more than 250 leading organisations.

ISF is governed by its members and managed by a professional management organisation.

Since 1989, ISF has invested over US$40 million in research.

ISF's past activities includes work on:

- information risk analysis;
- information risk management;
- security standards;
- risk management and corporate governance;
- cryptography and PKI;
- electronic commerce;
- external access;
- Internet security;
- network security;
- security administration;
- security organisation and management;
- technical architecture; and
- UNIX O/S and Windows O/S security.

Activities and ongoing work

During the next 18 months ISF's research will be focusing on the following areas:

- incident responses and incident management;
- return on investment;
- outsourcing;
- security and legislation; and
- identity management.

The ISF also publishes a *Standard of Good Practice in Information Security* and *Windows 2000 Security: Checklist Version 2* on its web site for people to download.

ISO/IEC 17799 UK Users' Group

The DTI acts as a facilitator for the ISO/IEC 17799 UK Users' Group. The UK group is an industry-led forum, with the business mission of promoting and disseminating the exchange of best practice and know-how of good information security management, based on the use of ISO/IEC 17799 and BS 7799 Part 2.

The group organises four workshops in London and across the UK each year.

Membership is open to any UK organisations using the 7799 standards or interested in using them. There is a mix of large and small companies, as well as a number of government departments and local authorities.

The DTI provides a secretariat for the group, compiling and issuing regular newsletters, maintaining a database of members and arranging steering committee meetings. There are some 560 members presently. The steering committee is composed of member companies. The DTI and British Standards Institute (BSI) also have seats.

Information about the group, including membership forms and details of forthcoming events, is available from the DTI achieving best practice web site.

In addition to the UK Users' Group, the Information Security Management Systems International Users Group (ISMS IUG) promotes understanding and awareness of the standards on an international basis. National Chapters have been established in 11 different countries, including Australia, Germany, Japan, Singapore, Sweden and the USA.

Jericho Forum
http://www.opengroup.org/projects/jericho

The Jericho Forum is an international circle of large IT user organisations dedicated to the development of open standards to enable secure, 'boundaryless information flows' across organisations.

'Boundaryless information flow' is a concept developed by the Open Group, a technology-neutral consortium of international vendors. It describes the ambition of achieving business-to-business networking facilitated by access to integrated information.

'De-perimeterisation' is the concept for how this can be achieved. The term encompasses the notion of protecting the individual data items, rather than putting protection around the perimeters of information systems, and includes all issues related to providing the security and architectures that support this.

The need for such standards had been growing for many years as organisations seek to exploit the business potential of the Internet and, at the same time, tackle the increasing problems of the security perimeter.

The Jericho Forum was formed at a meeting between an informal circle of users interested in de-perimiterisation issues and the Open Group management in January 2004. The Forum brings together large IT user organisations to explore the issues and to develop a set of definitions to clarify these terms.

Membership includes blue-chip companies in all major sectors of industry, including energy, banking, pharmaceutical, aerospace, postal, retail and government.

The group is in the process of developing formal governance processes. It is currently being managed by a temporary executive drawn from Royal Mail, BP and ICI.

Activities and ongoing work

The Jericho Forum activities are aimed at building business confidence to support the creation of boundaryless information flows. They focus on work to develop:

- cross-organisational security processes;
- shared security services; and
- products that conform to open source security standards and assurance processes that when used in one organisation can be trusted by others.

The Forum aims to be the channel through which the IT user organisations:

- define the problem;
- develop and communicate a collective vision;
- create the environment for innovation;
- demonstrate the market; and
- influence future products and standards.

A number of working groups are developing definitions of the business and technology issues associated with boundaryless business-to-business networking.

The Forum is also mapping out a timeline for the development of detailed standards.

It is also involved in the development of a White Paper on formal governance processes for boundaryless information flows.

National Computer Centre
http://www.ncc.co.uk

The National Computing Centre (NCC) promotes the effective use of information technology. It was established as a government organisation in 1966 and has about 1000 members.

During the 1980s NCC become an independent commercial operation. However, between 1996 and 1999, sell-offs and management buy-outs created new external companies in which the NCC no longer has any shares or equity. This allows the NCC to focus on its not-for-profit membership and research work and also to incorporate complementary membership organisations, including the Institute of IT Training, CICA (the Construction Industry Computing Association) and CIO-Connect.

Activities

The themes of NCCs activities are:

- compliance, security and risk management;
- e-business and knowledge management;

- standards, interoperability and open source; and
- programme management, skills and legal issues.

Ongoing work

NCC is developing guidelines for members and non-members on the following topics:

- software asset management;
- computer forensics;
- 'desert island' standards;
- managing risk;
- managing information security – certification to ISO 17799;
- e-risk management; and
- security in e-business.

A number of research projects have or will produce reports with recommendations to follow up:

- *Testing the Effectiveness of Security Measures 2002*;
- *Trust and Security for Easy Trade*;
- *National Security Vulnerabilities Survey 2003*;
- *SANS: BS 7799 Implementation Method*;
- *Operational Risk Standards for Compliance and Effective IT,* which includes the *IT Risk Management Survey 2003* and research with UMIST (University of Manchester Institute of Science and Technology); and
- *Survey of Information Security – Policy and Practice 2004*.

NCC is also carrying out work in the following areas:

- accreditation and certification for Bobby/W3C accessibility evaluation, the consumer assurance framework for electronic commerce and e-government interoperability, including some security issues;
- the development of best practice guidance on Risk Management and ISO 17799; and
- secure web development and hosting for local and central government (accredited), private sector and charities.

A number of events and training are planned on:

- BS 7799 implementation;
- computer forensics;
- assessing and mitigating risks to information assets;

- IT/governance;
- vulnerabilities briefings;
- trust and security;
- the MSc security module with the University of Manchester; and
- Internet vulnerabilities, scanning and reporting service.

Risk and Security Management Forum (RSMF)

The RSMF's web site is only accessible to members.

The Risk and Security Management Forum (RSMF) promotes professionalism in risk and security management. It provides a forum for members to discuss problems confidentially.

RSMF is a non-profit making organisation that was set up in 1990. Its membership is made up of 60 senior security practitioners and risk managers drawn from a wide range of commercial and industrial organisations, government departments, the armed forces, the Security Service and the police. In addition, there are a number of academics with an interest in crime prevention and public order.

Membership is by invitation only. Most members have a background at a senior level in the police, armed forces or the security service.

The RSMF meets four times a year to discuss topics of mutual interest and to exchange ideas and information.

All of the meetings are held under the Chatham House Rule. This means that members are free to use information discussed at the meetings, but cannot disclose the identity of other members or the organisations they work for.

Activities

RSMF uses the expertise of its members to:

- identify and communicate effective risk and security management;
- promote the benefits of effective risk and security management to senior executives;
- advise opinion formers in the public and private sectors on these issues; and
- develop inclusive ways of identifying, analysing, assessing, and controlling risk for the public and private sectors.

Information assurance is becoming a more significant part of RSMF work, particularly the areas of data centre protection – both physically and electronically and the impact of e-crimes on corporate brands, including market value.

Ongoing work

Four seminars are held each year on a wide range of information security-related topics. Recent subjects include the Government's counter-terrorist programme and Crown control in emergencies.

RSMF has run master classes for senior security professionals focused on communications and the human resources issues associated with response management of major terrorist attacks.

While these activities are aimed primarily at members, other senior security professionals are invited to attend.

SAINT (Security Alliance for Internet and New Technologies)
http://www.uksaint.org

SAINT is an organisation that develops and promotes awareness of best practice and methods to ensure security of Internet sites and new technologies.

It was founded in 2001 and is supported by several government departments, including the Cabinet Office and DTI. It is an independent, not-for-profit organisation that is governed by a constitution and executive committee.

The executive is limited to eight members. It currently includes representatives from the Cabinet Office, Confederation of British Industry (CBI), the Department for Trade and Industry (DTI), Microsoft, Intellect, IBM and Symantec.

In addition to these organisations, SAINT's membership is drawn from a number of leading vendors including, Sun, Oracle, Cisco, Nokia and Fujitsu.

A series of working groups, drawing together businesses in the same fields, analyses current practice and developments. There are currently three active working groups:

- The industry security web site working group aims to provide a vendor neutral portal for information assurance, highlighting best practice in Internet security.
- The 'return on investment' business case working group – which looks at the business benefits, including profitability, of spending to provide information assurance – is analysing how business cases for identifying information security risks and providing protection from those risks are presented.
- The education and training working group, which is assessing educational and training requirements for information security professionals.

Activities

SAINT achieves its objectives by carrying out specific projects, agreed by the executive at three-monthly intervals. The project work focuses on raising awareness of and developing and accrediting best practice in information security.

Ongoing work

SAINT is currently working with the Cabinet Office to assess information assurance in the UK within the public and private sectors.

It is also developing an online directory to support information security. Accessible on SAINT's web site, it provides links to external web sites and information portals to information assurance resources.

SAINT will produce a paper examining the need for professional accreditation of information security training and qualifications.

tScheme Limited
http://www.tscheme.org

tScheme is voluntary approvals scheme for electronic trust services that:

- defines standards of best practice;

- evaluates individual electronic trust services, including qualified certificate services, against those standards through an independent assessment process; and
- grants approval to trust services that continue to operate in accordance with the standards.

The 'tScheme-approved service mark' provides assurance to individuals and companies relying upon electronic transactions when choosing a service.

tScheme Limited was created in May 2000 and is an industry-led, not-for-profit, independent regulatory body for the emerging electronic trust services industry. It has a wide membership that includes trust services providers, technology companies, trade associations and potential relying parties.

Since then it has been the Government's preferred approach for fulfilling the requirements of Part One of the UK Electronic Communications Act 2000 (ECA). The CSIA, on behalf of the e-Government Unit and the DTI, supports the scheme and sends representatives to the tScheme Board meetings.

Activities

Since its formation, tScheme activities have focused on supporting the Government to deliver the key obligations of the Digital Signatures Directive (1999/93/EC). This includes supporting the development of capacity to regulate qualified certificate services.

Best practice approvals activity has expanded, in response to market demands for assurance in other forms of electronic identity credentials, including for use within 'closed user' group communities of interest. This is being developed alongside the original focus of commercially-provided PKI-based services.

tScheme has recently developed a new approval profile containing the criteria against which approvals may be granted to these new electronic identity services.

Ongoing work

tScheme plans to expand its membership to include:

- organisations belonging to 'closed user' groups in both e-business and e-government 'communities of interest'; and
- organisations with specific business requirements for secure online identity management.

tScheme will maintain its 'grant of approval' for digital certificate services, which will continue to award new grants of service approval. This will include the emerging electronic identity services that are initially expected to relate to e-government service intermediaries needing to establish a level of independent mutual assurance for secure online service delivery, such as the Local Authority Partnerships preparing to roll out e-government services from 2005.

A new scheme that will provide an independent standard of assurance for government PKI-based transactions between departments and agencies is currently in development.

'Criteria mapping' between tScheme, other forms of service assessment and existing information security standards will also continue. This work is to help applicants for approval to understand the criteria and evidence requirements before assessment and ensure that maximum accessibility is achieved for tScheme.

tScheme will continue work towards establishing a shared code of practice between voluntary 'electronic trust service' approvals schemes to help to support the future growth of secure international electronic transactions.

Industry groups for future consideration

This section provides an outline of the activities of a number of industry groups that were identified in the late stages of writing this report. SAINT plans to contact them to discuss their activities for inclusion in further editions of this report.

Internet Watch Foundation (IWF)
http://www.iwf.org.uk

The Internet Watch Foundation (IWF) was established in 1996 to take a partnership approach to tackle illegal material on the Internet, particularly the distribution of child abuse images, sometimes referred to as child pornography. The need to take this approach to deal with this crime was agreed between the Government, police and the Internet service provider industry.

Essentially the IWF provides a hotline for the public to report illegal or offensive material on the Internet. This can include:

- child abuse images;
- adult material that breaches the Obscene Publications Act; and
- criminally racist material.

The IWF works with law enforcement agencies in the UK or abroad to remove illegal content and prosecute offenders.

Interforum, e-Security Group
http://www.interforum.org/activities/group_e_security

InterForum is an independent, not-for-profit organisation working to ensure that the education, legislation and technologies are in place to help British businesses to profit from the digital economy.

A specialist group on e-security aims to:

- help create a secure environment for the use of information and communication technologies; and
- educate members, government and the wider business community on best practice e-security.

Institute of Directors, IT and e-Business Section
http://www.iod.com

The Institute of Directors (IOD) is a non party-political business organisation that was founded by Royal Charter in 1903. It has around 55,000 members. This includes the CEOs (Chief Executive Officers) of a number of large corporations, as well as entrepreneurial directors from many 'start-up' companies.

The IOD's web site has a section on e-business and IT. It includes details about their book *Secure Online Business*, which covers information risks, vulnerabilities and points of exposure on systems, software protection, security policies, organisational back-up and contingency planning.

ASIS International
http://www.asisonline.org

ASIS is an organisation for security professionals. It was founded in 1955 and has more than 33,000 members from all parts of the world. ASIS develops educational programmes and materials to help to improve security practices.

Additional groups whose activities will be identified for possible inclusion in future reports are:

Association of British Investigators
http://www.theabi.org.uk

Institute of Professional Investigators
http://www.ipi.org.uk

International Institute of Security
http://www.iisec.co.uk

Independent Information Security Group (IISyG)
http://www.informationsecuritysolutions.com/IISyg.htm

High Techology Crime Investigators Association
http://www.htcia.org

Association for Biometrics
http://www.afb.org.uk

European Biometrics Forum
http://www.eubiometricsforum.org

British Bankers Association
http://www.bba.org.uk

Foundation for Information Policy Research
http://www.fipr.org

Useful links

These links provide general information about information assurance from government web sites.

Cabinet Office

You can find out more about the government strategy for protecting critical information systems http://www.cabinetoffice.gov.uk/csia.

Communications–Electronics Security Group (CESG)

http://www.cesg.gov.uk provides advice and assistance on the security of communications and electronic data. CESG is part of the Government's National Technical Authority for Information Assurance.

Department of Constitutional Affairs

http://www.dca.gov.uk/foi/sharing/index.htm#part1a is the address for the DCA tool kit for the public sector on data sharing.

Department of Trade and Industry

You can find guidance on key information security issues, as well as details of all publications at www.dti.gov.uk/industries/information_security.

www.dti.gov.uk/bestpractice/infosec takes you to the DTI's Best Practice business advice pages.'

Home Office

http://www.homeoffice.gov.uk/crime/internetcrime/ gives you an overview of issues to do with Internet crime.

http://www.thinkuknow.co.uk/home.htm is run on behalf of the Home Office and offers advice and support on safe and effective use of the Internet.

http://www.identitytheft.org.uk/ is a web site produced by the Home Office Identity Fraud Steering Committee, a collaboration between UK financial bodies, government and the police to combat the threat of identity theft.

Metropolitan Police – Computer Crime and Internet-Related Crime

http://www.met.police.uk/computercrime/index.htm gives you information about what the Metropolitan Police is doing to respond to computer and Internet-related crime.

National Infrastructure Security Coordination Centre (NISCC)

http://www.niscc.gov.uk has information about services to protect the Critical National Infrastructure (CNI) from electronic attacks.

National Hi-Tech Crime Unit (NHTCU)

http://www.nhtcu.org tells you about the national policing response to hi-tech crime.

These are some additional links from private sector groups mentioned in this report:

APACS

http://www.chipandpin.co.uk/ tells you about the Chip and Pin Programme to increase the security of card transactions.

http://www.cardwatch.org.uk provides information for retailers, cardholders and the police to increase awareness of what they can do to prevent card fraud.

http://www.banksafeonline.org.uk helps consumers to bank safely.

British Chambers of Commerce

www.simplysign.co.uk is the British Chambers of Commerce site that has information about their authentication and trust services.

Information Security Forum

http://www.securityforum.org/html/frameset.htm allows you to download the Information Security Forum's *Windows 2000 Security: Checklist Version 2*.

Glossary of terms used in this report

Authentication

Authentication is the process of establishing the identity of computers, computer programs and users before they can perform any other system action.

Biometrics

This is the use of information and computer technology to verify the identity of a living person through the measurement of physical traits, for example, eye retina pattern.

Best practice

See 'security technology best practice'.

Bluetooth

Bluetooth is a communications standard that allows short-range wireless data communications. It provides a way to connect and exchange information between mobile devices; for example, laptop computers and mobile phones.

BS 7799 and ISO/IEC 17799

'ISO/IEC 17799 is an international (previously a British BS 7799) standard and is a code of practice for information security management.'They are defined by the British Standards Institution and the International Standards Organisation.

Business continuity

This term is used to describe the measures that an organisation takes to maintain normal business processes in the event of serious disruption. In the context of information assurance, disruption can be denial of service attacks, loss of data through viral attacks, and so on.

CERT

CERT, the Computer Emergency Response Team, issues warnings and security alerts about threats to computer and information technology. It is operated by the Software Engineering Institute at Carnegie-Mellon University (CMU). CERT was set up December 1988 by the Defense Advanced Research Projects Agency (DARPA) in the United States.

Certification

See 'digital certificates'.

Chief Security Officer (CSO)

This is the person in charge of all the staff and resources involved in maintaining security within a company, including information security.

Cyber Trust and Crime Prevention Project

This project is part of the Office of Science and Technology Foresight Programme. It explores the application and implications of next generation information technologies in areas such as identity and authenticity, surveillance, system robustness, security and information assurance and the basis for effective interaction and trust between people and machines.

DPA (Data Protection Act) 1984, amended 1998

The Data Protection Act set out principles to govern how data should be gathered and used, and how it should be protected from unauthorised copying and modification.

Data integrity

This is the assurance that data has been protected to prevent it from being changed in an unauthorised manner.

Data protection

This is the technology and procedures that protect the integrity and confidentiality of data. See 'data integrity'.

Digital certificates

Digital certificates assist authentication. They are issued to confirm identity and verify relationships when actions are performed within secure systems. See 'authentication'.

Digital signature

This is an electronic marker used to authenticate digital information and transactions. See authentication.

E-crime

This term is used to describe computer-based crime and criminal activity; for example, hacking, fraud and identity theft.

Encryption

This is the conversion of data or information into code to make it unreadable and keep it private during transmission or in storage. Decoding the data, converting the information into a readable form again, is called 'decryption'.

ENISA, the European Network and Information Security Agency

ENISA aims to ensure high levels of network and information security within the European Union. It assists the European Commission, Member States and their business communities in meeting the requirements of network and information security.

EU Framework Decision on data protection

This is a proposal for a pan-European law that will require communications services providers to keep user information for a minimum of 12 months.

Foresight Programme (Office of Science and Technology Foresight Programme)

The Office of Science and Technology is a unit within the DTI that leads for the Government in supporting science, engineering and technology and their uses to benefit society and the economy. The Foresight Programme produces science-based projects to provide challenging visions of the future to inform strategic development.

Governance

This is the process of managing business affairs.

Human factor issues

In biometrics, this refers to behaviour or physical traits, that are unpredictable or beyond the control of the biometric technology/application.

Information assurance

The confidence that information systems will protect the information they handle and function as they need to, when they need to, under the control of legitimate users.

Information infrastructure

This is a concept to describe all the elements that provide an electronic information network. The term embraces the hardware and software through which electronic and information services are provided. It includes telephone lines, cable systems, high-speed data networks.

Intellect

Intellect is the trade body for the UK based information technology, telecommunications and electronics industry.

Modem

Modem is short for modulator-demodulator. It is a device that enables computers to transmit data; for example, over telephone lines.

Open source code

A 'source code' is the specific set(s) of instructions – the programming language(s) and program(s) – that make computers operate and perform various tasks.

The term 'open' refers to making those sets of instructions widely accessible. Other individuals, organisations and companies are able to find out how the code works.

This allows the source code to be shared, improved, adapted, developed or modified to fix vulnerabilities by any individual or company.

One of the aims of providing open source systems is to increase the pace of technological advancement.

Phishing

This is online identity theft by the use of fake web sites and spoof e-mail, which assume the identity of legitimate organisations, to convince people to share their user names, passwords and personal financial information for the purpose of committing fraud.

PKI, public key infrastructure

Public key infrastructure, PKI, is the combination of hardware, software and procedures that allow the vetting and vouching of identities to provide authentication.

Public key

A 'public key' is numerical value used to encrypt data for transmission to a particular individual, who can decrypt is with a corresponding 'private key'.

Relying party

A relying party is an information system or user that relies on 'signed' data. See 'digital signatures', 'digital certificates' and 'authentication'.

RIPA (Regulation of Investigatory Powers) Act, Part 3

Part three of the Regulation of Investigatory Powers Act (RIPA) 2000 provides measures to help deal with the use by criminals of cryptographic and other information security technologies.

Risk management

This is the process of identifying, controlling, minimising and eliminating uncertain events that could disrupt business. The process includes assessing the risks, implementing security measures and evaluating systems put in place.

Security management

In the context of this report, security management is the process of identifying, controlling, minimising and eliminating vulnerabilities in information systems and processes. It includes assessing the risks, implementing information security measures and evaluating systems put in place.

Security technology best practice

This is the formal identification of successful methods, systems and procedures being used to provide secure technology.

Security architecture

A 'security architecture' is a framework of all the hardware, software, policies and procedures that are required to protect an information system.

SSL (Secure Sockets Layer)

SSL is an encryption procedure to provide secure communications on the Internet. It sets up a safe connection between the client and host on the Internet to allow the transaction of messages without the risk of data eavesdropping by third parties. The certificate verifies the server's authenticity.

USB, universal serial bus

This is a connection device for adding peripherals – printers, scanners, cameras – to personal computers.

Vulnerabilities

A vulnerability is a feature of an information system that can be used bypass security and protection measures.

Disclaimer

The author does not take responsibility for inaccuracies in this report. Neither does he endorse or offer any judgement on the quality of the work and activities of the groups mentioned in this report.

Copies of this report are available from:

CSIA
Cabinet Office
Stockley House
130 Wilton Road
London SW1V 1LQ

Tel: 020 7276 3267
Fax: 020 7276 5096
e-mail: csia@cabinetoffice.x.gsi.gov.uk
Website: http://www.cabinetoffice.gov.uk/CSIA