Global Information Assurance Certification Paper

UK Public Policy towards e-Commerce for Small to Medium Enterprises – An Information Security Perspective

Michael Johnson
7th December 2003
Practical Assignment Submission as part of GIAC Security Essentials Certification
Practical v1.4b Option 1

Table of Contents

1 - Abstract

In the United Kingdom (UK), the proportion of revenue generated by e-Commerce remains disappointingly small. Of those firms which do perform online transactions as part of their business processes, the majority are larger enterprises. Security concerns have been identified as being a significant inhibitor to the adoption of e-Commerce and security standards are markedly worse for Small to Medium Enterprises (SME's). It is perceived that a key to the future success of the UK economy lies in the use of the Internet as a central business tool by these organisations.

This paper looks at what is being done to address the poor state of information security as part of the strategy to encourage e-Commerce amongst this sector and what more could or should be done.

Section 2 outlines government policy towards e-Commerce and SME's. Section 3 reports current attitudes to information security and e-Commerce in this sector and investigates the extent of implementation of best practice security measures.

This paper highlights four key issues that need to be addressed by policy if the linked goals of greater take-up of e-Commerce and improved information security by SME's are to be achieved:

1. The need to convince SME's of the benefits of conducting business online.
2. The lack of confidence of both SME's and consumers in online transactions.
3. Lack of knowledge of those providing goods and services online on appropriate information security practice and of its significance.
4. Cultural change to accept the Internet as another transactional medium.

Section 4 takes a qualitative approach to assessing how effective a number of policies & other initiatives by the UK Government and institutions of the European Union (EU) are in addressing these 4 points.

Broadly, the conclusions are favourable though it is suggested that coordination of globally agreed standards by a supranational body should be implemented. Furthermore, it is concluded that enforcing certain standards by legislation should be considered.

2 - e-Commerce, SMEs and public policy in the UK and Europe

SME's are seen as the backbone of industrial activity in the UK and other European nations. They represent well over 90 % of enterprises in all European countries (97 % in the UK) and are key generators of new jobs and

innovators. However, many struggle to survive in the face of competition from larger organisations with greater marketing budgets and significant economies of scale.

E-Commerce is seen as a key to the future of European and UK economic strategy. It is also believed that this new business model will assist SME's to overcome some of their disadvantages of size using electronic shop fronts, e-Market places, and benefiting from cost savings resulting from new business models. These aims are behind the setting up of the Office of the e-Envoy at the heart of UK Government is focused on making the country the best place in the world for e-Commerce. Similar strategies are reflected at European level. The e-Europe Action Plan of 2002 was launched to implement the Lisbon Strategy agreed by the European Council of March 2000. The aim was to set a new goal for the EU in becoming the world's most dynamic and competitive knowledge based economy by 2010.

However, levels of trade conducted via the Internet and the numbers of firms adopting e-Commerce have been disappointing by most measures and figures have been particularly poor in the SME sector. The next section will look at the current status of Internet trading, at the significance of information security issues and at the relationship between the two.

3 - e-Commerce in the UK and Information Security Standards

3.1 - Status of e-Commerce in the UK.

A CBI (Confederation of British Industry) report in 2001 found that

> *"…although 70% of large firms with more than 10,000 staff are selling on the Internet, the figure drops to 20% of firms with less than 500 staff"*.[1]

As a proportion of all sales via any channel, only 1% of SME sales were made using the Internet in 2000.[2] There is certainly apathy towards e-Commerce which probably partly reflects sales volumes. In addition, according to a Department of Trade and Industry (DTI) sponsored report, only 19 % of all UK firms agree they thought they could save money with business to business (B2B) transactions with 26 % believing this would not save them money.

Research shows that consumer security concerns underlie the lack of consumer confidence in online transactions.

> *"A continued focus on earning consumer's trust and convincing them that it is easy and secure to transact online is necessary if the UK is to fully embrace the new economy."*[3]

[1] CBI Cybercrime Survey 2001
[2] Eurostat e-Commerce Database 2001
[3] DTI Information Security Breaches Survey 2002

In terms of business attitudes to e-Commerce, the CBI survey reveals that only half of the companies questioned believe that the Internet is safe for B2B transactions, and a little over 30% believe it is safe for business to consumer (B2C) transactions.

Table 3.1 Summary of stats presented in section 3.1
All figures are as a percentage of the sample surveyed.

Firms with more than 10,000 staff selling on the Internet 2001[1]	70%
Firms with less than 500 staff selling on the Internet 2001[1]	20%
Proportion of all UK SME sales via any channel, achieved using the Internet 2000[2]	1%
Proportion of all UK firms who believe they would save money with B2B transactions 2001/2 [3]	19%
Proportion of all UK firms who believe they would not save money with B2B transactions 2001/2 [3]	26%
UK companies who believe the Internet is safe for B2B transactions 2001 [1]	50%
UK companies who believe the Internet is safe for B2C transactions 2001[1]	30%

Any strategy to tackle the take-up of e-Commerce must therefore address consumer and business confidence in information security as well as showing tangible benefits to businesses. However, showing tangible benefits to business is intrinsically linked with improving confidence. This is because a lack of confidence detrimentally affects the volume of business and consumer online transactions. This in turn reduces the incentive for others to change business practice.

3.2 - Attitudes towards Information Security and levels of implementation of accepted Information Security good practice in the UK

According to the DTI survey[3], 44 % of companies in the UK were victims of malicious security breaches in the year to 2002. Despite this, according to the same report, whilst the number of UK businesses with a documented security policy has doubled since 2000, they still only account for 19 % of SME's against 59 % of large enterprises. In the same study, only 43 % of SME's had documented procedures to ensure compliance with the Data Protection Act (74% of large businesses). From a technical control point of view, a mere 61% of SME UK Web sites have a firewall in place to filter undesirable traffic coming into their Web servers from the Internet against 88% of large business sites[3] and only 58% of SME's encrypted messages passing over the Internet[3]. Finally, from an IT budget point of view, 34% of all firms did not allocate any expenditure to information security[3].

[1] CBI Cybercrime Survey 2001
[2] Eurostat e-Commerce Database 2001
[3] DTI Information Security Breaches Survey 2002

Yet from some perspectives, information security is seen as a major issue. In a European Commission report published in 2002 (data 2001)[1], security issues including those caused by viruses and hackers were seen as having at least some significance in business decisions to not have an Internet connection by 63% of SME respondents in the UK. However, when it comes to online transactions, the connection isn't made. This is reflected in the DTI report which suggests security is not seen as a major obstacle to implementing online transactions for e-Procurement, with only 17 % believing it was not straight forward to implement effective security for such systems[2]. However, an additional indicative figure here is that the majority of UK firms had little experience or no strong opinion. Ignorance about the subject would seem to be a reasonable explanation for these figures.

Table 3.2 Summary of stats presented in section 3.2
All figures are as a percentage of the sample surveyed. n/a = not available

	SME's	Large Enterprises	All Enterprises
Companies who were victims of malicious security breaches 2001- 2002[2]	n/a	n/a	44%
Companies with a documented security policy[2]	19%	59%	n/a
Companies with documented procedures to ensure compliance with the Data Protection Act[2]	43%	74%	n/a
UK Web sites with a firewall in place[2]	61%	88%	n/a
Companies encrypting messages passing over the Internet[2]	58%	67%	n/a
Companies not allocating any expenditure to information security[2]	n/a	n/a	34%
Companies seeing security issues as being a significant reason for not having Internet connectivity[1]	63%	78%	n/a
Companies believing it's not straight forward to implement appropriate to implement security measures[2]	n/a	n/a	17%

3.3 Summary of statistical study and implications for public policy

The issues raised in sections 3.1 and 3.2 suggest a need for government intervention to deal with a number of interlinked issues, many of which are related to education, but some of which are more to do with attitudes and culture.

Ultimately, if attitudes to conducting business over the Internet do not improve, neither will security standards. The surveys referred to in this paper suggest it is not seen as a being an integral part of the business. For example, the DTI report highlights the fact that 34% of businesses allocated none of the IT budget to security**Error! Bookmark not defined.**. This could be attributed to ignorance, and this may well be partly true. However, the perception of company web site as more of an 'add-on' is probably just as important in this respect. It could lead to the view that it does not deserve a serious budget, particularly as it often doesn't generate the same level of revenue as the rest of the business.

[1] Eurostat e-Commerce Database 2001
[2] DTI Information Security Breaches Survey 2002

Lack of confidence in e-Commerce security is linked with the issue of sales volumes, particularly from the consumer's point of view, many of whom will not buy over the Internet because they perceive it is not safe. If actual security standards do not improve, press reports of breaches will further dent confidence.

The need for a change in the way people view the Internet is a more intangible issue than hardening operating systems or implementing firewalls. Security risks are inherent in almost everything we do when making financial transactions, but purchasing online seems to worry people disproportionately to the risk. The example of people not being unduly worried by allowing their credit card out of their site in a restaurant is one often cited. Whilst it is true that e-Commerce security standards need to be improved, particularly amongst SME's, a shift in attitudes also needs to be encouraged before significant progress can be made.

Broadly summarised, then, initiatives should address the following 4 key issues:

1. The need to convince SME's of the benefits of conducting business online.
2. The lack of confidence of both SME's and consumers in online transactions.
3. Lack of knowledge of those providing goods and services online on appropriate information security practice and of its significance.
4. Cultural change to accept the Internet as another transactional medium.

The next section will compare a number of strategies being implemented at national and European level with the 4 requirements identified above.

4 – Analysis of Government Initiatives.

One initiative born of the EU strategy of 2002 towards making the Europe the world's most dynamic and competitive knowledge based economy is GoDigital. Its remit is to support e-Commerce ventures amongst SME's. In May 2002, a conference under took place in Brussels to discuss the progress of GoDigital and to make recommendations on future strategy. The views of the conference from a security perspective are summarised in the extract below:

> *The lack of confidence in the Internet is the main reason behind the under-development of e-Commerce amongst SME's. This is intimately related to the lack of awareness and skilled resources which altogether also explain why SME's have not equipped themselves with appropriate security technologies and processes.*
>
> *Both policy-makers and participants acknowledge the threats to security as a major barrier to the development of e-Commerce and e-*

Government services. In this respect, the Commission and the Council have taken a number of important steps to enhance the security of our EU communication and information networks. However, SME's seldom have financial or technical resources to dedicate to security.
Because of the lack of awareness on threats and risks to security, most SME's still need to be convinced of the benefits to address security now by investigating the risks, adopting available guidance and practices, and not as a remedial action. The major challenge is, therefore, how to develop in Europe a security culture, in particular towards SME's, and to facilitate the exchange of security best practices.[1]

The above extract appears to recognise at the European level, many of the 4 issues specified in section 3.3. However, practical measures are required to deal with them. The next sections will look at the following UK Government and EU initiatives as examples of public policy

- 4.1 - UK Government Office of the e-Envoy and the Government Gateway
- 4.2 – UK Online for Business
- 4.3 – Trust UK
- 4.4 - The UK Central Sponsor for Information Assurance
- 4.5 - The European Network and Information Security Agency
- 4.6 - The National High-Tech Crime Unit

These examples of policy implementation will use a qualitative analysis to compare with how well they address the four key issues identified in section 3.3 to come to conclusions about how successful policy is likely to be in resolving the interlinked issues of e-Commerce popularity amongst SME's and security:

1. The need to convince SME's of the benefits of conducting business online.
2. The lack of confidence of both SME's and consumers in online transactions.
3. Lack of knowledge of those providing goods and services online on appropriate information security practice and of its significance.
4. Cultural change to accept the Internet as another transactional medium.

4.1 - UK Government Office of the e-Envoy and the "Government Gateway"

The UK Government has taken a lead in the arena of online transactions and doing business over the Internet, in setting up the Government Gateway under the control of the 'Office of the e-Envoy' (OeE). The OeE's aim is

[1] eEurope: SMEs GoDigital Conference Report 2002

> "*to improve the delivery of public services and achieve long term cost savings by joining up online government services around the needs of customers. The e-Envoy is responsible for ensuring that all government services are available electronically by 2005 with key services achieving high levels of use.*"[1].

The Office was set up with the slogan "Leading the Drive to get the UK Online" in September 1999, when the ambitious deadline for enabling electronic access to government services was set. Currently, it is possible, amongst other things to submit Value Added Tax (VAT) returns, perform income tax self-assessments; apply for export licences and to apply for certain social security benefits. This is all performed through the central Government Gateway [2] with a single sign on.[3]

The government must take credit for taking the lead in promoting the benefits of online transactions in this project. This is despite initial criticisms of restricting the solution implemented by Microsoft (inevitably) to Microsoft products[4] . A subsequent report recognised the benefits of Open Source products including the security benefits of system diversity. [5] From the point of view of setting an example in the area of Information Security practice, one of the key parts of this organisation is the Security and Authentication Unit. The following paragraph describing this organisations' areas of work illustrates sound principles in this area:

> *"The Security and Authentication area of work covers; enabling trust, authentication and secure transactions across government and the wider economy; providing universal access, by enhancing take-up of, and trust in, electronic services. Current activities include; supporting the Cabinet Office initiatives to introduce the information security standard BS7799; trust guidance for the OeE strategy of wider Internet access through new technologies and applications."*[6]

To reinforce this point, the e-Envoy site also provides access to framework documents that specify policy and security requirements for e-Government; continuity of business; protection from malicious attack and how to achieve assurance on system compliance with security policy. [7]

This is a widely recognised strategy for encouraging businesses to move towards implementing new business models based upon Internet enabled systems. An EU GoDigital report put it like this:

---

[1] Office of the e-Envoy Home page.
[2] Government Gateway Homepage.
[3] Security is provided in the form of 128-bit SSL connection, encryption, digital certificates for certain transactions or User ID Authentication.
[4] Linuxuser. "Microsoft.gov.uk ?"
[5] Office of the e-Envoy. Report. "Open Source Software Use Within UK Government."
[6] Office of the e-Envoy "Trust and Security in e-Government"
[7] Office of the e-Envoy "Frameworks and Policies for the Development of e-Government

> *"The case of the US under the Clinton administration is an illustration of such a process: the setting up of a federal on-line procurement system urged American SME's to go digital. The same would happen in Europe*."[1].

The idea is to show the practical applications by giving businesses and consumers access to useful services online.

This initiative would seem to have benefit from the point of view of tackling 3 of the 4 key issues. Firstly, by taking the lead, the Government is attempting to lead cultural change whilst (secondly), demonstrating the benefits of online transactions to businesses as well as citizens. Thirdly, the fact that good security practices seem to be applied in providing these services should ensure confidence in such transactional methods.

4.2 – UK Online for Business

UK Online[2] was set up by the e-Envoy's office as an umbrella organisation for initiatives to promote e-Commerce, e-Government and e-Citizen. UK Online for business was set up to cover any government activity in support of business. It represents a partnership between industry and government and provides a one stop shop, aimed at SME's. All online services are provided free of charge.

These include impartial business-focused advice about information security and e-Commerce in general from commercially independent government backed business support organisations. Advisers are accredited in a scheme administered by the Chartered Management Institute and anyone taking part in the scheme must be re-accredited annually.

E-commerce showcase events are also organised around the country. Acting as networking as well as demonstration events, they allow SME's to share experience and see demonstrations and presentations of practical applications of e-Commerce.

UK Online for Business also attempts to tackle the issue of poor implementation of information security good practices by making a number of online sources available to businesses[3] Subjects include information on threats, an Information Security Glossary, and information on standards such as BS7799. In addition, it provides an online Health Check assessment[4] which covers all the main areas of good practice:

- Security Policy.
- Security Organisation.

[1] eEurope: SMEs GoDigital Conference Report 2002.
[2] UK Online for Business Homepage
[3] UK Online for Business Information Security Resources
[4] UK Online for Business Information Security Healthcheck

- Asset Classification and Control.
- Personnel Security.
- Physical and Environmental Security.
- Communications and Operational Management.
- Access Controls.
- System Development and Maintenance.
- Business Continuity Management.
- Compliance.

Within each category, more in depth questioning leads to an overall assessment allowing an organisation to determine those areas requiring attention.

Finally, a link to the UNified Incident Reporting and Alert Scheme (UNIRAS), the UK Government's Computer Emergency Response Team[1] provides the latest in threat information to organisations.

A study published in 2002 by the European Commission compared the merits of various e-Commerce policies and initiatives directed at SME's. In its assessment of UK Online for business, it said:

> *"UK Online for business is a well targeted policy with a strong political commitment. It uses a wide range of instruments and the programme has also adapted to change during its lifetime, shifting towards helping businesses to make more sophisticated use of e-business.... and greater effort has been put into tailoring case studies and promotional and awareness raising activities for different regions and sector-focused activities. There is also a strong involvement of the private sector"*[2]

To summarise, UK Online for Business is aimed at a number of the 4 key issues affecting e-Commerce popularity and information security. It addresses the requirement to convince SME's of the applications and benefits of e-Commerce by providing real-life examples and staging events allowing SME leaders to network with peers. In addition, by providing advice, checklists, and access to certified advisers, it also attends to the need for education and raising the profile of information security issues.

4.3 – Trust UK

Trust UK is firmly targeted at consumer confidence. It is a non-profit organisation endorsed by the UK government which establishes minimum standards of trading, information security and treatment of personal data for participating organisations. Companies trading online use its distinctive logo as a sign of membership, which aspires to be the online equivalent of the British Standards Institution's Kite Mark in establishing a recognisable symbol

[1] UNIRAS Homepage
[2] European Commission, Benchmarking e-Business Policies for SME's

that you can have confidence in making a transaction on a participating Web site.

As a concept, it deals with the trust and confidence issues of B2C enterprises, though Trust UK suffers from a lack of publicity. Despite its aspirations, it is not a widely recognised scheme.

4.4 - The UK Central Sponsor for Information Assurance

The Central Sponsor for Information Assurance (CSIA) was set up in October 2002 as a unit of the UK Government's Cabinet Office. Its role is to work with both the public and private sectors, and international counterparts as a coordinating body, to provide

> *"…a central focus for information assurance in promoting the understanding that it is essential for government and business alike to maintain reliable, secure and resilient national information systems.*
> *The CSIA will encourage a 'culture of security' regarding information systems across central and local government, the private sector as well as to the general public."* [1]

One of its initiatives is an accreditation scheme to promote a variety of assured products that the public [and private] sector can use.

The CSIA is a backbone organisation in promoting standards in information security and as a coordinating body. In this respect, it is crucial for building confidence in online transactions, another key requirement in addressing issues affecting e-Commerce.

However, whether it is sufficient to promote a 'culture of security' is debateable as it leaves open the option of organisations ignoring its role. The question of whether legislative requirement would be appropriate arises here.

Furthermore, on its home page, CSIA states that it

> *"works with partners in the public and private sectors, as well as it's international counterparts, to help safeguard the nation's IT and telecommunications services"* [1]

However, it is not clear how the relationships with international counterparts work. Given the international nature of the Internet and threats to security, a common supranational[2] approach is imperative.

4.5 - The European Network and Information Security Agency

[1] CSIA Homepage
[2] Transcending national boundaries

The European Network and Information Security Agency (NISA) is due to come into operation in January 2004. Its objective is:

> *"to create a common understanding in Europe of issues relating to information security that is necessary to ensure the availability and security of networks and information systems in the (European) Union."*[2]

Essentially it is a coordinating and awareness raising body, similar to the CSIA, though at a European level, allowing improved security information exchange. Part of its remit is to act as a supranational advisory body. It is also designed as a single point of contact for non-European states on security issues.

The starting point of this initiative was the recognition of the importance of networks and information systems to business, consumers, government and citizens and the efforts being made by member states of the EU to improve security. The issue prompting the setting up of NISA was the recognition of variations in progress between governments, and differences in approach as well as the lack of cross-border cooperation and the fact that security threats do not recognise international borders. Furthermore, it was recognised that there was need for an effective and coordinated response to security threats. Linked to these issues are the differing legal frameworks within countries relating to information security and regulatory standards causing a lack of interoperability which decreases the effectiveness of security products and services.

Reaction to this new organisation has been mixed. Whilst its remit was broadly welcomed, the make-up of the board was criticised as being too heavily weighted towards EU officials. Calls were made for increased industry involvement[1].

However, it must be welcomed as it deals with criticism of a lack of a trans-national approach to standards and confidence in online transactions across borders, albeit without legislative back-up. This is approach is demonstrated in the proposal document which outlined the terms of establishment of NISA:

> *"In June 2002 the OECD adopted their Guidelines for the Security of Information Systems and Networks…. These guidelines emphasise the importance of applying certain common principles for information security and underpin the work that is taking place on a European level"*[2]

4.6 - The National High-Tech Crime Unit

[1] http://www.vnunet.com/News/1141650

[2] European Commission , Proposal for Establishing the European Network and Information Security Agency

The National High-Tech Crime Unit's (NHTCU) remit is to

> *"combat national and transnational serious and organised hi-tech crime within or which impacts upon the United Kingdom"*[1].

It emphasises the confidential nature of any reports of incidents in order to protect the reputation and brand of victims.

It is an important part of the requirement to build confidence with businesses and consumers that security issues are taken seriously and as a deterrent to cyber crime. However, in a sense, the involvement of this body is a sign that preventative measures have failed so the public emphasis should be on prevention.

5 Conclusion

The volume of online business transactions as a proportion of total sales for SME's is low in the UK. Lack of confidence in security standards is cited time and time again as a reason for not buying online by consumers and many businesses. The perception of the Internet as an insecure transactional medium is backed up by the evident poor quality of security standards implemented, particularly by SME's. These factors together leave the reputation of the Internet as vulnerable as the systems which comprise it.

There are a number of government initiatives, based upon strategies for encouraging SME's to move towards greater adoption of Internet enabled business models. They are aimed at B2B as well as B2C enterprises and go some way to addressing the 4 key issues specified in section 3.3 towards the linked objectives of improving information security standards and e-adoption.

Central to the ambitious e-Government (Government Gateway) project is an attempt at shifting cultural attitudes to e-Commerce by business and consumers. Meanwhile, UK Online for Business attempts to educate firms, particularly SME's of the virtues of good system security and what good practice means, whilst promoting the real commercial benefits of e-enabled business. To address issues of confidence, the consumer orientated Trust UK is an attempt at providing an instantly recognisable standard of integrity, privacy and security of transactions.

The CSIA was set up in partnership with industry to encourage common standards of information assurance. By encouraging public and private organisations to use the same standards, (assuming they implement them), confidence can be built. However, ultimately, standards must be agreed upon at a global level & with a supranational body as guardian and or enforcer. Common standards are vital in a medium where security issues do not respect international borders. Currently, the CSIA is reflected at European

[1] NHTCU Homepage

level by NISA which in turn follows guidelines set by the OECD. This is a model which should be built upon.

Finally, whilst great efforts are being made to address information security issues and popularity of Internet based electronic transactions, it may be that a legislative approach will be needed to force application of good practice. It is application of good practice which will prove crucial to EU and UK dreams of a digital society.

Definitions of abbreviations and concepts

Abbreviations

- B2B – Business to Business
- B2C – Business to Consumer
- CBI – Confederation of British Industry
- CSIA – Central Sponsor for Information Assurance.
- DTI – Department of Trade and Industry
- EU - European Union
- NISA – European Network and Information Security Agency.
- NHTCU – National Hi-Tech Crime Unit
- OeE – Office of the e-Envoy
- OECD – Organisation for Economic Cooperation and Development
- SME - Small and Medium Enterprises – Commercial organisations employing up to 250 people
- UK – United Kingdom
- UNIRAS – Urified Incident Reporting and Response and Alert Scheme
- VAT – Value Added Tax – UK Purchase tax.

Concepts

- e-Commerce – Refers to commercial Internet transactions in their broadest sense, that is the method used to place or receive the order, not the payment or the channel of delivery.
- Supranational – Transcending national boundaries (e.g. authority, or organisation)
- Transnational – Extending beyond national boundaries

References

Bennett, M "EU Crime Unit Under fire" IT Week 16 June 2003. As reported on vnunet URL: http://www.vnunet.com/News/1141650

CBI, Fraud Advisory Panel, PricewaterhouseCoopers, Armor Group and International Fraud Prevention Research Group. "Cybercrime Survey 2001." 2001. As reported by Goodwin, W. "CBI warns on cybercrime." Computer Weekly 15 September 2001
URL: http://www.computerweekly.com/Article106118.htm (14 November 2003)

eEurope, GoDigital, "SMEs – Europe's Future, eEurope: SME's GoDigital Conference Report." June 2002 URL: http://europa.eu.int/information_society/topics/ebusiness/godigital/docs/conference_docs/godigitalconferencefinalreport.pdf (12 November 2003)

European Commission. "Benchmarking national and regional e-business policies for SMEs" Final Version. 12 June 2002
URL: http://europa.eu.int/comm/enterprise/ict/policy/benchmarking.htm (16 November 2003)

European Commission. "Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency" Final Version. 11 February 2003 URL: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2003&nu_doc=63 (20 November 2003)

Eurostat, "e-Commerce Database 2001." 2001. Figures published by European Commission, Eurostat. "E-Commerce in Europe, Results of Pilot Surveys carried out in 2001." July 2002
URL:
http://europa.eu.int/comm/enterprise/ict/studies/lr-e-comm-in-eur-2001.pdf (30 November 2003)

HM Government CSIA. Homepage
URL: http://www.cabinet-office.gov.uk/csia/ (17 November 2003)

HM Government, Department of Trade and Industry, PricewaterhouseCoopers, "Information Security Breaches Survey, 2002" 2002
URL: http://www.ukonlineforbusiness.gov.uk/cms/resource/file/dti_survey.pdf (14 November 2003)

HM Government. Government Gateway Homepage. URL: http://www.gateway.gov.uk/ (12 November 2003)

HM Government Office of the e-Envoy. "Frameworks and Policies for the Development of e-Government"

URL: http://www.e-envoy.gov.uk/Resources/FrameworksAndPolicy/fs/en (15 November 2003)

HM Government Office of the e-Envoy. Homepage
URL:http://www.e-envoy.gov.uk/Home/Homepage/fs/en (12 November 2003)

HM Government Office of the e-Envoy "Open Source Software Use Within UK Government." Version 1. 15 July 2002.
URL: http://www.govtalk.gov.uk/documents/oss_policydocument_2002-07-15.pdf (15 November 2003)

HM Government Office of the e-Envoy. "Trust and Security in e-Government"
URL: http://www.e-envoy.gov.uk/Responsibilities/Security/fs/en (15 November 2003)

HM Government UK Online for Business. Information Security Healthcheck
URL: http://www.ukonlineforbusiness.gov.uk/healthcheck/index.jsp (16 November 2003)

HM Government UK Online for Business. Homepage
URL:
http://www.ukonlineforbusiness.gov.uk/cms/template/mainhome/310360.htm (16 November 2003)

HM Government UK Online for Business. Information Security Resources
URL: http://www.ukonlineforbusiness.gov.uk/cms/template/infor-security.jsp?id=212908 (16 November 2003)

HM Government. UNIRAS Homepage
URL: http://www.uniras.gov.uk (16 November 2003)

Linuxuser "Microsoft.gov.uk ?" Issue 11. June 2001.
URL: http://www.linuxuser.co.uk/articles/issue11/gateway.html (15 November 2003)

Trust UK Homepage
URL: http://www.trustuk.org.uk/Default.asp (17 November 2003)

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