***SIBIS***
IST–2000-26276
Statistical Indicators Benchmarking the Information Society

# SIBIS – Workpackage 2: Topic research and indicator development

## Topic Report No.3: Trust and Security

Tasks 2.1 (Update) + 2.2

| | |
|---|---|
| Report Version: | Final |
| Report Preparation Date: | Dezember 2001 |
| Classification: | Restricted |
| Authors: | Lorenzo Valeri, Leon Cremonini (RAND Europe) |
| Contract Start Date: | 1st January 2001 |
| Duration: | 30 Months |
| Project Co-ordinator: | empirica (Germany) |
| Partners: | Work Research Centre (Ireland), Danish Technological Institute (Denmark), Technopolis (UK), Databank Consulting (Italy), Stichting RAND Europe (Netherlands), Fachhochschule Solothurn (Switzerland) |

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

# Table of Contents

# 0 Overview

One of the enabling elements of creating an information society in Europe is a fast and secure Internet. In this "secure" should not only be seen in terms of secure technology, but wider then that: both technical security measures as perceived security ("trust") by consumers and organisations. The first part of this document presents a general overview of policy literature and statistical indicators as they are existing and accessible today. Thereby, it provides the basis for identifying the gaps: which information would we need from a policy perspective, and which is lacking? Together with exploring the existing indicators we therefore will develop a vision on which indicators would complement the policy need for information.

The fulfilment of the eEurope aims (as well as any other aim, in fact) needs the consideration of two questions: "Where do we stand?" and "Where must we go?". Answering these questions is essential and can be afforded only through a adequate set of reliable indicators.

The policy literature review, summarising the most important policy findings and including a definition of key terms, highlights the main issues at stake concerning security and trust:

- Rising number of individuals on-line
- Borderless character of the Internet
- Economic impact and number of organisations suffering attacks
- Characteristics of the victims of cyber crime and of its perpetrators
- Variety of crime types due to the ever-changing aspect of the Internet
- Law enforcement and new legal initiatives to deal with new forms of criminal offences linked to the Internet
- Technical capability of the Internet to cope with authentication and protection
- Awareness of trust and security issues
- Ability to deal with trust and security issues (Training and education)

The underlying analysis commences with a review of a list of policy documents at national and supranational level. This leads to an overview of specific issues arising in the current policy debate.

Looking at both supranational and national level is important, as it is only very recently that supranational collaboration on the issue of trust and security takes place. Whereas there is already some experience in this on law enforcement level (i.e. exchange of information and collaboration between police forces) security has remained predominantly a national issues. Therefore looking at national level issues is crucial, since they are based on a longer history and deeper insights: considering the supranational level is crucial since trust and security on the Internet is a global issues and cannot be achieved by single countries alone.

On top of achieving a better comprehension to what extent national contexts influence the issues emerging (therefore emphasising the relativity of such issues) it is also possible to assess the achievements of different governments on defined eEurope goals. Referring to Security and Trust, we can then discover, for example, that the most concerned about national security issues are the US and France, while Germany appears as the leading nation in the defence of human rights, as far as these are under a new (subtler) threat linked to the Internet. The UK is, instead, the paladin of the need of industry to take voluntary measures (against cyber crime and attacks), while noting at the same time that the government should be ready to take legislative action if necessary[1].

Of course these themes indicate states' tendencies, not their only concern.

1 The fact that certain issues fit one national case rather than an other is not incidental. However, this matter goes beyond the purposes of the SIBIS project.

Finally, we explore a list of existing (traditional and innovative) indicators, with a glance to what should come next - that is identifying gaps and suggesting possible indicators further to be developed in D 2.2.

The second part presents a methodology to define standardised indicators to measure trust, confidence and security in the context of information society. It opens by arguing for the need to move away from seeking a single benchmark metric for trust, confidence and security. Instead, it presents the case for concentrating on defining three distinct indicators for security.

As a basis for indicator development, **security** is defined as *the combination of technical and managerial processes that aim to foster confidentiality, privacy, integrity & availability of data and information systems, as well as to provide authentication and non-repudiation functionalities*.

The analysis then concentrates on the identification of the **units of analysis**, which should guide data collection based on surveys and existing indicators. Finally, the report examines the three single indicators that should be used as the security benchmark:

- Online Malicious Activities
- Prevention of Malicious Activities and Downtime
- Online Interaction Facilitators

Particular attention is given to identifying possible approaches for combining traditional and innovative indicators in order to derive a single aggregate measure. However, the report concludes by arguing that the three indicators should be kept separate. The reason is that they cannot be homogenised or compared unless they are quantified using a common base.

# 1 Introduction: Issues and Concepts

## *1.1 Aims of Deliverable 2.1*

Concerns about security of electronic networks and information systems have been growing along with the rapid increase in the number of network users and the value of their transactions. The perception of insufficient protection by citizens is a potential impediment to the development of the Information Society, since they will not use the Internet if they feel threatened in their privacy. New sorts of crimes are emerging, using the tools of the Information Society. At the same time, there may be a trade-off between security and privacy, since the more accessible the site is the less personal information its visitors need to submit in order to download or upload materials and responses. Consequently, however, this means that the greater amount of privacy one desires can be achieved only at the price of less accessibility.

The topic going to be discussed here is exactly “Security and Trust”, important under a policy perspective as far as it arises the question on how an Information Society can be developed, and, at the same time, assure citizens with an adequate amount of security, gaining their confidence.

The general aims of the deliverable (here with reference to “Security and Trust”) are the following:

- Provide an in-depth description of Topic areas (i.e. the results of Topic research activities);
- Review published literature concerned with “Security and Trust”, in order to realise both the main issues currently relevant to this topic and the existing indicators;
- List issues and dimensions that require the development of *new* indicators.

The work of Deliverable 2.1 is consistent with the general aims of SIBIS, because:

- Describing the results of the Topic research activities (largely explicated in WP1) is an essential first step if we want to take stock of existing statistical concepts and data sources to check their suitability to meet users' requirements, as aimed at by the SIBIS project;
- As previously stated, insufficient security (or this sort of perception) is a threat to the development of the Information Society. Since one of the main goals of SIBIS, taking full account of the e-Europe action lines, is to contribute to policy making in this area through the development of indicators for benchmarking progress towards the Information Society, reviewing published literature and listing issues and dimensions requiring the development of new indicators (in this specific case addressed to "Security and Trust") appears a necessary starting point for the development of new indicators. This activity will take place in Deliverable 2.2 (Part 2 of this document).

## *1.2 Description of work tasks*

The main activity of Deliverable 2.1 is a "Topic research", in order to provide a well-structured and concise overview of the "state of the art" in the topic of competence (in this case "Security and Trust"). Through this activity WT 2.1 will identify main policy issues and existing indicators relevant to these issues, highlighting also the gaps to be filled[2].

The work will largely rely on literature review of policy documents and scientific publications. Therefore, it will strongly be based on WP1 (mostly WT 1.2 and WT 1.3), starting point and input to WP2: policy documents described in WT 1.2 of WP1 will be considered and re-analysed, as well as statistical documents described in WT 1.3 of WP1.

Deliverable 2.1 will comprise the following work tasks:

- Setting down a report on the topic research activities
- Setting down a list of most relevant issues and key dimensions of the Information Society for which new statistical indicators are to be developed
- Proposing a set of definitions for required statistical indicators along the lines of the e-Europe objectives.

Foundation and ratio of these tasks are the "eEurope action lines" as expressed in the "e-Europe Action Plan: an Information Society for All". On the "Trust and Security" side, such action lines are taken into deep consideration while addressing WT 2.1, conscious of the vital role secure networks and access (with the improved public trust that flows from them) have in building the Information Society. In particular this section is most concerned with the action lines relevant to "Security and Trust" such as improving security of any on-line transaction and developing a co-ordinated European approach to cybercrime.

## *1.3 Structure of the First Part*

the first part of this report is divided into 6 main sections:

1. The current introduction, aimed at offering a general overview of the work.
2. A literature review based on Ch. 1.3 and 1.4 of WP 1. Flowing from the contributions offered in these parts of WP 1, this chapter goes in greater depth, extrapolating the key

[2] This is the starting point of WT 2.2, where new indicators will be developed.

issues as they emerge from statistical documents relevant to security and trust. A second part of the review is engaged in highlighting the existing indicators (which allowed us to raise the fundamental issues previously mentioned), without, however, describing them in detail, since this will be a task of Ch. 4. Finally, a definition list of key terms is supplied.

3. A policy documents review, concerned mainly with policy documents relevant to security and trust as they emerge from Ch. 1.2 of WP 1. While an overview of the documents is offered, also a brief description of the contents and objectives is given, as they emerge from WP 1 (mainly the document abstracts). The review is split up in 3 paragraphs, relevant to the different areas of interest within the security and trust topic:
   - Policy documents at a European level
   - Policy documents at a national level
   - Relevance of these documents for the SIBIS project as a whole
4. A review of existing indicators. The chapter is engaged in the identification of indicators presented in Ch. 2 of this WP as well as the gaps. Such work appears to be the inevitable starting point for Deliverable 2.2, where new indicators will be developed on this basis.
5. A final outline of the Topic report's findings that offers a summary of what emerged in the chapter. Its goal is to draw the attention on the relevant issues raised in order to point the way forward to the work of Deliverable 2.2, which will be aimed at translating policy concerns into a coherent set of Information Society indicators for each of the nine topics.
6. The concluding section of the Deliverable is a detailed bibliography of the sources used.

# 2 Literature review

One of the most perceptible impacts of eEurope has been on the legislative process. Governments and administrations, including the Commission, have recognised that the 'new economy' and particularly the Internet, pose challenges to the legislative framework. The Internet is a cross-border medium where new ways of doing business are developing. It is very quickly changing the market context and the de facto 'rules of the game', posing problems for issues like data protection, information security, taxation and consumer protection which require immediate solutions. The current process of drawing up legislation needs to be accelerated. eEurope and, in particular, its endorsement by the European Councils in Lisbon and Feira, has helped to raise awareness and the Council and the European Parliament have made major efforts to accelerate the process. Therefore, *Security problems,* both real and perceived, are widely seen to be an inhibiting factor for the development of the Information Society, with particular reference to e-Commerce.

A Eurobarometer survey conducted for eEurope in Autumn 2000 found that around 17% of all Internet users had experienced certain problems. The majority of these related to receiving too many unsolicited E-mails (9%)[3]. These jumped to 15.1% during year 2001[4], according to a similar Eurobarometer survey conducted in spring of this year. However, this appears to be more an intrusion of privacy than a security threat. Viruses, instead, are a major security issue and these were encountered by around 8% of users[5], which rose to 11.4% in 2001[6]. Credit card abuse was experienced by only around 2% of users in 2000[7] and decreased to 0.9% the following year[8].

[3] Source: FLASH EB N°88 «Internet et le Grand Public» (10-30/10/2000) – Rapport, p. 18, available at http://europa.eu.int/ISPO/basics/measuring/eurobaro/eurobaro88/docs/Eurobarometre-Oct001.pdf
[4] Source: FLASH 97 : « INTERNET ET LE GRAND PUBLIC » - 02/2001, Volume A, p. 6, available at http://europa.eu.int/information_society/eeurope/benchmarking/list/source_data_pdf/tables_by_ms.doc
[5] Source: FLASH EB N°88
[6] Source: FLASH 97
[7] Source: FLASH EB N°88
[8] Source: FLASH 97

The main issue at stake is, then, what solutions can/should be envisaged for threats of this kind. Technology cannot provide all the answers to what are problems posed by humans. If "vulnerability" can be seen primarily as a technical issue, this is not necessarily the case for the information security domain as a whole. As a matter of fact, the latter is often much more a business and management issue rather than a technical one. The answer to the dilemma is to adopt tried and tested measures to counter specific threats facing organisations and to build these into day-to-day business operations. Moreover, individual concerns about privacy, security, and the use of information about their preferences and activities are an important barrier to the formation of an effective and broad-based information society. If individuals distrust sending the identifying or financial information over the Internet that is needed to complete transactions, the fraction of commercial and societal activities which can benefit from transition to the electronic medium will be significantly restricted. As a result, insufficient protection (or a perception of insufficient protection) of personal privacy and security in these systems is a potentially serious impediment in the development of the information society and, therefore, is important from the policy perspective.

It appears clear, then, that security and trust are pivotal elements in the development of the e-Economy and the Information Society, and important issues emerge when attempting to achieve such goals.

The following sections highlight two aspects of the topic. In 2.1 the main issues, emerging from relevant literature. will be considered, while 2.2 deals more specifically with the indicators emerging from that literature and defines some key terms necessary to have a better understanding of such indicators.

## *2.1 Main issues from the literature*

### 2.1.1 Issues Relevant To The Topic Under Discussion

#### *Awareness*

*Concerning general information Security*

Great financial losses need to raise the level of information security awareness, which remains scarce. According to UK statistics ISBS 2000 (a UK based quantitative survey) over 30% of organisations do not consider information concerning their business as critical and/or sensitive in nature[9] (in most cases, a company that considers information concerning their business as critical and/or sensitive in nature has already suffered a major breach). This problem emerges also because of the lack of a common way of valuing information. As far as there seems to be a good state of information security awareness in the market place addressing "high profile" security issues, such as viruses and passwords, nevertheless the awareness and understanding of what can be done to combat the more significant risks, particularly those posed by human actions, and those arising from doing business electronically is still insufficient[10].

People tend to blame ITs for any sort of problem, but in many cases one should point his finger at "digital illiteracy". Often – but not always – information security is seen only as an issue for the IT department, which it clearly is not. *Good information security management is about organisations understanding the risks and threats they face and the vulnerabilities in their information and network infrastructures. It is about putting in common-sense procedures to minimise the risks and about educating all the employees about their responsibilities. Most importantly, it is about ensuring that the policy on information security management has the commitment of senior management.*

[9] Source: DTI, Communications and Information Industry Directorate, Information Security Breaches Survey, 2000 Technical report, available at http://www.dti.gov.uk/cii/datasecurity/survey2000techreport

[10] *Ibid*.

Relying on the government to secure your communications is clearly not sufficient: although collaboration between industry and government is crucial, since industry owns most of the information infrastructure and its underlying infrastructures and is responsible for securing its own systems, but, for instance, cannot pursue perpetrators and also has a role in protecting critical infrastructures, at large.

A major problem at the level of the individual organisation is the absence of an Information Security Management System. It is only when these procedural and management issues have been addressed that organisations can decide on what security technologies they need and thus adequately secure their own systems. For an information security management system to be effective, it must address three key areas:

- Definition of the aims and objectives of information security. A policy that has the commitment of senior management;
- Assessment of the security risks. A policy that is grounded in a risk assessment process. A process that considers the value of the information and other assets at risk and balances this against the spending on security controls. A process that reviews the risk periodically to take account of changing circumstances and new risks;
- Selection and implementation of controls.

*Concerning legislation*

UK data (ISBS) show a low awareness (25%) of the legislation currently in force and best practice guidelines, which do exist[11]. This could be linked to the education issue
This can be linked to the FBI's idea about "law enforcement". The main problem here is how to enforce the current laws, according to the FBI, which participated to the annual survey conducted by CSI (Computer Security Institute) *Computer Crime and Security Survey*. However a major problem (as emerges in the UK) is the ignorance on what these laws are, what they prescribe, and how they can protect citizens/organisations from e-Crime[12].

### *Training and education*

This issue is strongly linked to that of awareness. How can organisations defend themselves against the new forms of cybercrime? By being aware of these risks (issue 1). But how does one raise awareness? According to the above quoted CSI annual survey technologies and policies are not enough, but

> *[…] organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and the technical dimensions. They also need to properly fund, train staff and empower those tasked enterprise-wide information security13.*

The education issue seems to be crucial since threats of cybercrime are empowered by ignorance. First of all, there is a need to be "digitally literate" to have awareness of such threats.

Moreover, as will be noted when considering the national cases, the issue of awareness and training is strongly related to national defence and security matters[14].

### *Borders*

The problem emerging from the data here is the (new) possibility of being victim of a criminal located thousands of miles away (or to commit a crime at this distance). How can/should states fight these new forms of crime? In what way can/should they be measured in order to be able to give a common (international) response?

---

11 *Ibid*.

12 Source: Computer Security Institute, press release concerning the 6th annual "Computer Crime and Security Survey.", Financial Losses due to Internet Intrusions, Trade Secret Theft and other Cybercrimes, San Francisco, March 12, 2001, available at http://www.gocsi.com/prelea/000321.html

13 *Ibid*.

14 See Ch. 3, case of USA

The IFCC (Internet fraud complaint Centre of the US) data show how, at least at the US level, only a minority of fraud via the Internet originates and ends in the same state. The "Six-Month Data Trends Report: May 8-November 8, 2000", highlights the truly borderless character of the phenomenon. In California, for example, where most fraud seems to originate, only 22.2% of referred cases involve both a complainant and a perpetrator residing in the same state, while in Georgia this percentage drops to 4.3%, by far the lowest in the US.[15] Similarly, the National Fraud Information Centre (USA National Consumers League), by means of the statistics developed by their "Internet Fraud Watch", observe that the problem of bounderless crime through the Internet is increasing : 3.5 % of Internet fraud complaints in the US was addressed to Canadian companies (year 2000). Complaints against other states was lower. However they significantly more than doubled between 1999 and 2000 (from 1% to 2.3%)[16].

### *Victim's characteristics*

Data of the IFCC (Internet Fraud Complaint "Centre of the US) relevant to the semester May-November 2000 show that most complaints come from males (71.3%) aged in their mid-thirties (26.6%, while individuals aged between 40 and 49 comprise, according to these statistics, 25.1%). They also usually lose more money than other complainants (average loss of male victims, for instance, is 330 US$ against 140 US$ of females)[17]. This may tell us that females, the elderly and poorer sections of the population access the Internet at a lower degree, therefore risking an exclusion from participating to the Information Society. It must be said, however, that the IFCC gathers complaints via the Internet, thus raising the point of its actual representativeness of the general population.

### *Law enforcement*

Data from the US (for example the annual CSI survey, quoted above) suggest that little is done to enforce existing legislation, which could be applied to new forms of crimes. In the US, the FBI has established, as attempted solutions, an Infrastructure Protection Centre (NIPC) and Regional Computer Intrusion Squads.

### *"Overpopulation" on line*

According to the American "Internet Fraud Watch", the US have seen a 600% increase in complaints since 1997. This trend is also confirmed at a European level (for example by Eurobarometer data). Questions which may arise from such data are the following (for example)

- Are there more crimes?
- Is there more awareness about these new forms of crime?
- Is it due to the growth in numbers of Internet users?

Moreover, what consequences will the full realisation of the Information Society have?

### *Fraud types*

The issue here is the ever growing number of different cybercrimes. It is difficult to classify "fraud types" due to the novelty of such crimes and the fact that their point of strength lays in the ignorance and unawareness of the general public. A categorisation has been attempted by the IFCC (Internet Fraud Complaint Centre), presented also in the definitions of key terms, yet it must constantly be updated.

---

[15] Source: Internet Fraud Complaint Center (IFCC), Six-Month Data Trends Report, May-November 2000, p. 10, available at http://www1.ifccfbi.gov/strategy/6monthreport.PDF

[16] Source: National Fraud Information Center, Internet Fraud Watch 2000, available at http://www.fraud.org/internet/lt00totstats.htm

[17] Source: Internet Fraud Complaint Center (IFCC), Six-Month Data Trends Report, May-November 2000

*Size of the organisation*

The ISBS 2000 UK based survey seems to build a direct correlation between the size of the organisation and its information protection systems: the greater the enterprise is the better data protection it has. This raises two points:

- Is "cyberthreat" directly proportional to the "size" of an organisation? If yes, what do we use as a scale of "size" for different organisations?
- How costly is the introduction of good practices against e-Crime? Is the fact that bigger firms are better defended against such breaches, a signal of an unaffordable price to introduce protections for smaller firms? Or is it just a sign of greater awareness of big firms due to their being greater victims

## 2.2 Indicators from the Literature

*Indicators in the Trust and Security area include the following*

- Consumer perceptions about trust and security;
- Levels of security threats and security compromises that are occurring;
- Economic impacts of consumer concern about trust and security;
- Economic impacts of commercial practices which, while raising privacy concerns, promote efficiencies and generate economic profits;
- Economic impacts of ICT security breaches for governments, firms, and individuals;
- Presence of the infrastructure and related products associated with increasing overall security and trust;
- Nature of all company practices addressing these issues; and
- Enforcement of government and company policies and practices addressing these issues.

Data about citizens' perceptions about security and privacy issues surrounding both the Internet and the use of other information technologies can be gathered through traditional survey instruments. Information on consumer perceptions about security, privacy and trust need to be complemented, as much as possible, with indicators of real conditions in this area.

## 2.3 Data sources

The main sources for data on indicators mentioned in this document are:

1. ISBS 2000 (Information Security Breaches Survey 2000). A UK based quantitative survey conducted using a structured questionnaire across a demographically representative range of organisations in the UK. It must be reviewed on 2001/07/31.
2. IFCC (Internet Fraud Complaint Centre): Six-month data trend report. It is a compilation of information on complaints received and referred by IFCC (USA) to law enforcement or to regulatory agencies for appropriate action. (May-November 2000).
3. Computer Crime and Security Survey (2001). Annual survey by the American CSI (Computer Security Institute)
4. Internet Fraud Watch (2000). Statistics based on Internet surveys in the US.
5. CERT/CC (CERT Co-ordination Centre) Statistics. American Centre of Internet security expertise. It provides statistics on incidents handled, vulnerabilities reported, security alerts and notes published, hotline calls handled, and email messages handled
6. Understanding the Digital Divide. The data presented here are taken from the work of the OECD's Directorate for Science, Technology and Industry (DSTI) and are part of an ongoing OECD effort to measure the extent of the "digital divide".

7. Eurobarometre (Flash 97)
8. Polizeiliche Kriminalstatistik (Statistical document on crime in Germany. It considers various sorts of criminal offences, among which also computer crime)
9. Michael Floria, Rolf Lurs and Malte Lehman-Jessen, "The Future of Security and risks in Telecommunication-Expectations of Experts-(TeleDephi)", Report of a Dephi survey conducted in Germany concerning the future of information security and risks. Report published in Gunter Muller and Kai Rannenberg, Multilateral Security in Communications, (London: Addison Wesley, 2000), pp. 465-481
10. Pew Internet Report, The Internet Life Report: Trust and Privacy Online-Why Americans Want to ReWrite the Rules, Final report, August 2000
11. UK National Consumer Council, E-Commerce and Consumer Protection, London, August 2000
12. Consumers International, Privacy @ Net, an International Comparative Studies on Consumers' Perception about Privacy Online, January 2001
13. Consumers International, Should I Buy?: Shopping Online 2001: An International Comparative Study of Electronic Commerce, September 2001

## *2.4 Definition of Key Terms*

1. Security and Privacy: The more accessible the site, the less citizens or visitors are obliged to provide personal information in order to easily download or upload material and responses
2. Communication Infrastructure: the collection of hardware equipment and procedures (software, management) for transporting data needed by an application to deliver specified services to the users. Synonymous with information infrastructure.
3. Complex system: collection of a large number of functional entities (equipment, procedures and humans) with a large number of interconnections among them.
4. Vulnerability: weakness or flaw in the system that eliminates or reduces its ability to deliver the specified services, or (in the context of critical infrastructures) is related to interdependencies between systems due to massive interconnections in systems-of-systems
5. Identity Theft: the appropriation of somebody's identity by using information collected over the Internet or other ways and means in order to commit a specific set of frauds. In this information age, identity theft is often the starting point of these specific kind of frauds described in the following sections.
6. Financial Institution Fraud: Knowing misrepresentation of the truth or concealment of a material fact by a person to induce a business, organisation, or other entity that manages money, credit, or capital to perform a fraudulent activity. Credit/debit card fraud is an example of financial institution fraud.
7. Gaming Fraud: to risk something of value, especially money, for a chance to win a price when there is a misrepresentation of the odds or events. Sports tampering and claiming false bets are two examples of gaming fraud.
8. Communications Fraud: a fraudulent act or process in which information is exchanged using different forms of media. Thefts of wireless, satellite, or landline services are examples of communications fraud.
9. Utility Fraud: when an individual or company misrepresents or knowingly intends to harm by defrauding a government regulated entity that performs an essential public service, such as the supply of water or electrical services.
10. Insurance Fraud: a misrepresentation by the provider or the insured in the indemnity against loss. Insurance fraud includes the "padding" or inflating of actual claims, misrepresenting facts on an insurance application, submitting claims for injuries or damage that never occurred, and "staging" accidents.

11. Government Fraud: a knowing misrepresentation of the truth, or concealment of a material fact to induce the government to act to its own detriment. Examples of government fraud include tax evasion, welfare fraud, and counterfeit currency.
12. Investment Fraud: deceptive practices involving the use of capital to create more money, either through income-producing vehicles or through more risk-oriented ventures designed to result in capital gains. Ponzi/Pyramid schemes and market manipulation are two types of investment fraud.
13. Business Fraud: when a corporation, or business knowingly misrepresents the truth or conceals a material fact. Examples of business fraud include bankruptcy fraud and copyright infringement.
14. Confidence Fraud: the reliance on somebody else's discretion and/or a breach in a relationship of trust resulting in financial loss. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. Auction fraud and non-delivery of payment or merchandise are both types of confidence fraud.

# 3 Policy Documents

## *3.1 Overview Of Policy Documents On Trust and Security*

| Title of document | Region | Publication date | Type of document* |
|---|---|---|---|
| 1. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data | OECD | 1980 | Documentation |
| 2. Guidelines for the Security of Information Systems | OECD | 1992 | Documentation |
| 3. Guidelines for Cryptography | OECD | 1997 | Documentation |
| 4. Guidelines for Consumer Protection in the Context of Electronic Commerce | OECD | 2001 | Documentation |
| 5. ComCrime Study | EU | 1999 | Documentation |
| 6. Study on the Legal Issues Relevant to Combating Criminal Activities Perpetrated Through Electronic Commerce | EU | 2001 | Documentation |
| 7. Public hearing on Creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer related crime. | EU | 2001 | Other |
| 8. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime | EU | 2001 | Documentation |
| 9. Draft Convention on Cyber-crime and Explanatory Memorandum Related Thereto | Council of Europe | May 2001 (draft) | Documentation |
| 10. Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime | EU | 2001 | Documentation |
| 11. Council Decision to Combat Child Pornography on the Internet | EU | 2000 | Documentation |
| 12. Speech of Erkki LIIKANEN “Trust and security in electronic communications: The European contribution" | EU | 2000 | Other |
| 13. Action Plan on Promoting Safer Use of the Internet | EU | 1999 | Action Plan |
| 14. Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures | EU | 1999 | Documentation |
| 15. eEurope 2002. Impacts and priorities. A communication to the Spring European Council in Stockholm, 23-24 March 2001 | EU | 2001 | Report |

| Title of document | Region | Publication date | Type of document* |
|---|---|---|---|
| 16. eEurope: an Information Society for all. Communication on a Commission Initiative for the Special European Council of Lisbon, 23-24 March 2000 | EU | 2000 | Report |
| 17. Communication from the Commission “Realising the European Union’s Potential: consolidating and extending the Lisbon Strategy | EU | 2001 | Report |
| 18. Communication from the Commission “Network and Information Security: Proposal for a European Policy Approach” | EU | 2001 | Report |
| 19. eEurope action plan: “An Information Society for all” | EU | 2000 | Action Plan |
| 20. Commission Study “Unsolicited Commercial Communications and Data Protection” | EU | 2001 | Other |
| 21. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain legal aspects of Information Society service in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’) | EU | 2000 | Documentation |
| 22. Opinion 5/2001 On the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH | EU | 2001 | Documentation |
| 23. Recommendation 1/2001 on Employee Evaluation Data | EU | 2001 | Documentation |
| 24. Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union | EU | 2001 | Documentation |
| 25. Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000 | EU | 2001 | Documentation |
| 26. Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act | EU | 2001 | Documentation |
| 27. Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons | EU | 1998 | Other |

| Title of document | Region | Publication date | Type of document* |
|---|---|---|---|
| 28. Conference documents: From User to Citizen: "The Citizen and the Global Information Society | EU | 1998 | Report |
| 29. “Public Strategies for the Information Society in the Member States of the European Union” | EU | 2000 | Report |
| 30. Common Criteria for Information Technology Security Evaluation | Inter-national | 1999 | Documentation |
| 31. Electronic Communication Bill | UK | 1999 | Documentation |
| 32. Promoting Electronic Commerce (July 1999) | UK | 1999 | Documentation |
| 33. Federal Act Establishing the General Conditions for Information and Communication Services – Information and Communication Act- (*Informations- und Kommunikationsdienste-Gesetz- IuKDG-* | Germany | 1997 | Documentation |
| 34. Act on the Protection of Personal Data Used in Teleservices- Teleservices Data Protection Act- (*Teledienstedatenschutzgesetz- TDDSG-*) | Germany | 1997 | Documentation |
| 35. Law Governing Framework Conditions for electronic signatures and Amending Other regulations | Germany | 2001 | Documentation |
| 36. Innovation and Jobs in the Information Society of the 21st Century | Germany | 1999 | Action Plan |
| 37. Trusted *e*Commerce | Germany | 2001 | Report |
| 38. Projet de loi sur la société de l’information | France | 2001 | Documentation |
| 39. Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique | France | 2001 | Documentation |
| 40. Mise en oeuvre du Programme d'action gouvernemental pour la société de l'information – Etat d'avancement après un an (janvier 1998 - janvier 1999) | France | 1999 | Other |
| 41. Directive n. 4201/SG Sécurité des systèmes d’Information | France | 1995 | Documentation |
| 42. Computer Security Act | USA | 1987 | Documentation |
| 43. Presidential Decision Directive/NSC-63 | USA | 1998 | Documentation |
| 44. National Plan For Information Systems Protection | USA | 2000 | Action Plan |
| 45. Cyber Security Information Act | USA | 2000 | Documentation |
| 46. Road map for National Security: Imperative for change | USA | 2001 | Report |
| 47. Unique Health Identifier for Individuals – A white paper | USA | 2001 | Report |

| Title of document | Region | Publication date | Type of document* |
|---|---|---|---|
| 48. Uniform Standards for Patient Medical Record Information, report to the Secretary of the US Department of Health and Human Services | USA | 2000 | Report |
| 49. National Committee on Vital and Health Statistics Report to Secretary Shalala for the period 1996-1998 | USA | 1998 | Report |

* Categories: Report, Documentation, Green Paper, Action Plan, Evaluation, Other

### *1. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

The guidelines, adopted on September 23, 1980, were intended to help to harmonise national privacy legislation and, at the same time, prevent interruptions in international flows of data. They still represent a basis for actions in this field.

### *2. Guidelines for the Security of Information Systems.*

The guidelines, adopted in November 1992, provide a set of principles aimed at enhancing the security of information systems. They also call for activities in the field of public awareness, education, technological and economic development and international cooperation. Following an initial revision in 1997, these Guidelines are presently being examined by the OECD in order to assess their continuous effectiveness in this Internet age.

### *3. Guidelines for Cryptography*

These guidelines, adopted in 1997, provide a list of principles suggesting possible national and international regulations about cryptography. The most important aspect of this document has been the explicit separation between the use of cryptographic solutions for encryption purposes and its exploitation for devising digital signatures. The document has also called for the increased liberalisation of the export of cryptographic products and systems.

### *4. Guidelines on Consumer Protection in the Context of Electronic Commerce*

These guidelines, which have been adopted in 2000, clearly state a set of principles aimed at protecting consumers who are engaging on business-to-consumer activities. They do not specifically address security issues. Nevertheless, they address concerns and issues (delivery failures, redress, dispute resolutions) that consumers consider essentially if they are expected to develop trust and confidence towards online commercial activities.

### *5. ComCrime Study*

Drafted by Prof. Ulrich Sieber of the University of Wiezburg, the ComCrime study was presented at the European Council in Tampere in 1999. It provides an overview of the different substantive and procedural legal procedures related to computer-crime. It also provides interesting suggestions and courses of actions to counter this phenomenon in the future. In particular, it calls for harmonisation of substantive and procedural legal measures, the establishment or strengthening of computer crime units, and larger investment in training and research and development.

### *6. Study on the Legal Issues Relevant to Combating Criminal Activities Perpetrated through Electronic Commerce*

Drafted by researchers from Queen Mary and Westfield College of the University of London, it builds on the ComCrime studies. However, the authors have conducted a several survey concerning the attitude and perceptions of communication service providers (CSPs) operating in Europe. Particular attention was devoted to issues such as access to stored and protected data and control of content and communication data in general. Specific recommendations have been put forward. This report has been part of the supporting activities leading to the drafting of the Commissions' communication concerning computer-related crime, which is examined in point 7.

### *7. Public hearing on Creating a Safer Information Society by improving the Security of Information Infrastructures and Combating Computer related*

The hearing represents a comment in the Commission Communication "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", and sets the way forward to contrast Internet related crime and let the Commissions inputs effectively come true.
Policy objectives:

- Law enforcement and mutual recognition
- Industry co-operation (while causing them minimum burden)
- Respect of privacy to be preserved

### *8. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*

This Communication discusses the need for and possible forms of a comprehensive policy initiative in the context of the broader *Information Society* and *Freedom, Security and Justice* objectives for improving the security of information infrastructures and combating cyber-crime, in accordance with the commitment of the European Union to respect fundamental human rights.

Policy objectives:
- Preventive technologies
- Enhancement of public awareness
- Substantive procedural and legislative provisions
- Creation of trained law-enforcement personnel
- Co-operation between different actors
- Combat child pornography

### *9. Draft Convention on Cyber-crime and Explanatory Memorandum Related Thereto (May 2001)*

The Draft addresses the need for harmonised substantive and procedural legal measures aimed at countering cybercrimes, which are not already addressed through other traditional offline legal instruments. It is the end result of a long period of international cooperation supported by the Council of Europe aimed at countering cybercrime, which started in 1989. The preparation of this draft has also directly involved non-Council of Europe members such as Australia, Japan

Policy objectives:
- Definition of a set of measures to be taken at the national level concerning cybercrime, in particular:
  - Illegal access

- Illegal interception
- Data Interference
- System Interference
- Computer-related Offences (forgery, fraud)
- Content-Related Offences (pornography and copy-right violations)

• Definition of procedural measures aimed at countering and prosecuting these cybercrime

### *10. Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime*

EU Working Party on Data Privacy issues this opinion. This organisation, which was established by the 1995 EU Directive on Data Privacy, re-united data/information protection commissioners of the Member States. In this opinion, it has expresses a set of concerns about potential impact of the proposed convention on cybercrime on data privacy. In particular, it wanted to

• To emphasise the role of the Council of Europe in defending fundamental rights and freedoms (privacy and personal data protection first of all), while promoting international co-operation in combating cyber-crime.
• To clarify the text of the articles of the draft convention because their wording is often too vague and confusing and may not qualify as a sufficient basis for relevant laws and mandatory measures that are intended to lawfully limit fundamental rights and freedoms

### *11. Council Decision to Combat Child Pornography on the Internet*

This decision wants to combat child pornography on the Internet.

Policy objectives:
• Co-operation between different states and with industry
• Awareness of Internet users
• Exchange of existing expertise
• Creation of expertise in the field of fighting child pornography on the Internet

### *12. Speech of Erkki LIIKANEN "Trust and security in electronic communications: The European contribution"*

The speech underlines the absence of an adequate degree of security in the Networks and privacy protection, which causes a lack of trust by users who, therefore, often remain potential.

Policy objectives:
• Reinforce competition in the Telecommunications market.
• Lower Internet Access tariffs
• Stimulate broadband access offers.
• Complete the Internal Market for *e*-commerce
• have a minimum level of common rules within the EU
• facilitate cross-border *e*-commerce within the Internal Market,
• Give legal guarantees to consumers and businesses.
• Enhance actual use/knowledge of these technologies

### *13. Action Plan on Promoting Safer Use of the Internet*

Within a span of four years (Jan. 1, 1999 – Dec. 31, 2002), the Action Plan wants to promote a safer use if the Internet environment and encourage, at a European level, an environment favourable to the development of the Internet industry.

Policy objectives:

- Promotion of industry self-regulation
- Help the implementation of adequate systems of self regulation
- Content-monitoring schemes
- Public awareness
- International co-operation
- Exchange of experiences and best practices at European and international levels;
- Pump prime developments by supporting demonstrations and stimulating application of technical solutions;
- Alert and inform parents and teachers, in particular through their relevant associations
- Promotion of co-ordination across Europe and between actors concerned
- Ensure compatibility between the approach taken in Europe and elsewhere

### *14. Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures*

Directive dealing with legal aspects of e-signatures.
Policy objectives:

- Facilitate the use of electronic signatures
- Provide for the non-differentiation between hand-written and electronic signatures as long the technical and procedural requirements indicated in the four annexes are fulfilled.
- Contribute to legal recognition of electronic signatures
- Establish a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the Internal market

### *15. eEurope 2002: Impacts and priorities. A communication to the Spring European Council in Stockholm, 23-24 March 2001*

Evaluation of the impact and priorities of the eEurope actions. Aim to accelerate the development of the information society in Europe and to ensure its potential is available to everybody - all Member States, all regions and all citizens.

Policy objectives:

- To accelerate the development of the information society in Europe
- To ensure its potential is available to everybody - all Member States, all regions, all citizens.

### *16. eEurope: an Information Society for all. Communication on a Commission Initiative for the Special European Council of Lisbon, 23-24 March 2000*

Communication that takes into account the EU actions to address the gaps of the eEurope initiative.

### *17. Communication from the Commission "Realising the European Union's Potential: consolidating and extending the Lisbon Strategy*

This report presents a picture of progress since Lisbon and highlights areas where action must be accelerated or extended.

Policy objectives:

- Create more and better jobs
- Create new European labour markets – open to all, with access for all
- Economic reforms for goods and services
- Integrated financial markets
- Achieve the right regulatory environment
- *e*Europe 2002 (knowledge-based economy)
- Digital literacy and improving the skills base in the EU
- Develop research, innovation and enterprise
- Capture the next wave of knowledge technologies ("frontier technologies")
- Effective social protection for ageing population

### *18. Communication from the Commission "Network and Information Security: Proposal for a European Policy Approach"*

This Communication wants to be a response to the request of the Stockholm European Council of March 23-24, 2001 to develop a comprehensive strategy on security of electronic networks including practical implementing action.

### *19. eEurope Action Plan "An Information society for all"*

Communication on a Commission Initiative for the Special European Council of Lisbon, 23-24 March 2000.

### *20. Commission Study "Unsolicited Commercial Communications and Data Protection"*

Commission study on "spam" (unsolicited commercial E-mails), with focus on legal and ethical aspects of violation of privacy, as well as a comparison between the EU and the US on this phenomenon, how to contrast it and how it is perceived.

### *21. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of Information Society service in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*

This Directive is concerned with certain legal aspects of Information Society (information to be provided, identifiability of commercial communications etc.) with the aim of insuring the fee movement of information society between the Member States.

### *22. Opinion 5/2001 On the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH*

This Opinion by the Data Working Party (EU advisory body on Data Protection and Privacy), addresses the issue of personal data protection and public access to documents within the Community institutions and bodies

### *23. Recommendation 1/2001 on Employee Evaluation Data*

This recommendation by the Data Working Party addresses the issue of privacy, offering an explanation of the definition of "privacy" given in Directive 95/46/EC, as "[…] not only […] resulting from objective factors […] but also any other element, information or circumstance having an information content such as to add to the knowledge of an identified or identifiable person."

### *24. Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union*

This Recommendation by the Data Working Party, aims to contribute to the effective and homogeneous application of the national provisions adopted in compliance with the personal data protection Directives, by providing concrete indicators on how the rules set out in the Directives should be applied to the most common processing tasks carried out via the Internet.

### *25. Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*

Opinion by the Data Working Party, considering the Australian Privacy Amendment Bill of December 6, 2000, under a European perspective. While welcoming it as a whole, the DWP looks with concern at the fact that certain sectors and activities are excluded by the act (employee data and Small business), and addresses the gaps.

### *26. Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*

This opinion of the Data Working Party analyses the Canadian Personal Information and Electronic Documents Act of April 13, 2000 addressing its limitations/gaps as well as potentialities.

### *27. Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*

This study has the following aims:

- Examine the situation in EU Member States with regard to protections of legal persons
- Describe the risks to the free movement of data within the Internal market
- To make recommendations concerning legal persons as opposed to individuals

### *28. Conference documents: From User to Citizen: "The Citizen and the Global Information Society*

The focus is on issues raised in the Discussion Paper in order to identify the strategies that need to be followed in Europe to protect European business, economy, culture and societal values.

Policy objectives:

- To create a legal framework which enhances and protects existing democratic rights (privacy protection, democratic structures, etc.);
- To establish practical rules of engagement which will encourage people to use new technologies (quality content, easy access and reasonable tariffs);
- To promote awareness of the real opportunities available for the citizen (work, education, health, environment, new services etc);

- To ensure that products and markets meet the highest standards to satisfy consumer needs (intellectual property, common technical standards, choice of products and services etc.)
- Avoid social exclusion

### *29. "Public Strategies for the Information Society in the Member States of the European Union"*

The report provides an overview of the public strategies for the information society in the Member States of the EU, taking into account the past, current and proposed initiatives.

Policy objectives:
- Information Society as a major priority
- Awareness and wide spread use of ICT
- Limited intervention by governments
- Develop digital skills
- Enhance accessibility
- Enhance confidence

### *30. International Standard (IS) 15408-Common Criteria for Information Technology Security Evaluation*

This international standard allows for the independent testing and evaluation of the security functionalities of products and systems. It also allows for organisations to draft and have evaluated "protection profiles", which indicates a set of security functionalities that are expected to be provided by a specific tools. Presently, a large number of states have subscrived mutual evaluation arrangements which allows product evaluation and certifications completed in one country to be automatically recognised by other signing parties. It is expected to slowly replace other security evaluation and certification standards, Europe's Information Technology Security Evaluation Criteria (ITSEC) and the US Trusted Computer System Evaluation Criteria (TCSEC).

### *31. Electronic Communications Bill*

This Bill was adopted in 1999, and has the aim to facilitate the use of electronic communications and electronic data storage, confer powers to require the disclosure of data needed to obtain access to electronic information or to make it intelligible, to make provision about the modification of licenses granted under the Telecommunications Act of 1984.

### *32. Promoting Electronic Commerce*

This paper contains both, an invitation for comments on the Government's proposals for an Electronic Communications Bill, and explanatory notes on the Bill, and the Bill's draft. It also explains the government's aims with passing this bill.

Policy objectives:

- facilitating electronic commerce
- targets for the government facilities available on-line: 25% by 2002, 50% by 2005, and 100% by 2008.
- 90% of routine government procurement of goods to be done electronically by 2001.

### *33. Federal Act Establishing the General Conditions for Information and Communication Services – Information and Communication Act- (Informations- und Kommunikationsdienste-Gesetz- IuKDG*

This Act of 1997 is still referred to in Germany as an essential document for subsequent legislation. Its purpose is to establish uniform economic conditions for the various applications of electronic information and communication services.

### *34. Act on the Protection of Personal Data Used in Teleservices- Teleservices Data Protection Act- (Teledienstedatenschutzgesetz- TDDSG-)*

Act issued by the Federal Government to set a legal framework on the conditions for electronic commerce.

### *35. Law Governing Framework Conditions for electronic signatures and Amending Other regulations*

This normative document is concerned with electronic signatures and sets conditions for their use in the safest conditions.

The purpose of the Law is to create framework conditions for electronic signatures, introducing, where necessary, additional conditions for the use of qualified electronic signatures for public administrative activities, based on objectivity, proportionality and non-discrimination.

### *36. Innovation and Jobs in the Information Society of the 21st Century*

This action Programme covers the activities needed to launch Germany's move into the information age, addressing the following aims:

- Increase the spread of information and communications technologies
- Ensure the inclusion of all social groups
- Safeguard the interests of the general public and protect human dignity
- Adapt educational/training systems
- Increase research in the area
- Expand the IT infrastructures
- Increase the spread of innovative forms of work
- Ecological modernisation through the new technological potentials
- Increase the efficiency of the public sector through communication technologies
- Promote co-operation at a European and broader international level

### *37. Trusted eCommerce*

The document considers *e*Commerce and m-Commerce tackling in particular the issue of security, considering it a matter not only of the transmission technology, but also the organisation of "Trusted *e*Commerce-Systems. The question of security is of particular relevance and is considered in some depth.

### *38. Projet de loi sur la Société de l'information*

This text has the aim of regulating the access to information and archives but also freedom of communication on-line, it sets juridical rules on electronic commerce and access to the net as well as norms dealing with security in the information society.

### *39. Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*

This decree, in application of the law of March 13, sets down in four chapters a regulation concerning electronic signatures.

Policy objectives:

- Avoid falsifications
- Avoid fraud
- Respect of privacy

### *40. Mise en oeuvre du Programme d'action gouvernemental pour la société de l'information – Etat d'avancement après un an (janvier 1998 - janvier 1999)*

The document is divided in seven chapters, dealing with different aspects of the information society in France. Chapter 6 considers specifically the regulation frame and legal matters, and touches explicitly the issue of cyber-security (6.3)

Policy objective: Assure the safety of the national network information systems

### *41. Directive n. 4201/SG Sécurité des systèmes d'information*

The aims of the directive (which still represents an important milestone in French policy) are:

- To indicate the path to follow with respect to the information systems in France
- To outline the objectives to follow
- To define the organisations responsible for the achievement of these objectives

### *42. Computer Security Act*

This Act of 1987 still represents a starting point and an "inspiration" for further action. The purposes of the Act are to provide guidelines to assure cost-effective security and privacy of sensitive information in Federal computer systems, and to assure periodic training for the persons involved.

### *43. Presidential Decision Directive/NSC-63*

PDD 63 is mainly concerned with protection of critical infrastructures and data protection, considered basic elements of the nation's strength.
Policy objectives:

- Vulnerability Analyses
- Remedial Plan based upon the vulnerability assessment
- Establishment of a national warning centre to warn of significant infrastructure attacks
- Development of a system of response to infrastructure attacks
- Education and Awareness
- Research and Development
- Development and implementation by the Intelligence Community of a plan for enhancing collection and analysis of the foreign threat
- International Co-operation
- Evaluation of legislative and budgetary requirements
- Dissemination

The first version of the Plan largely focuses on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures.

Policy objectives:

- Achieve a critical information systems defence with an initial operating capability by December 2000
- Protect the private information of its citizens that resides on its computers
- Computer Security and Privacy (Ensure public access to data)
- Efficiency (Maximising the use of information collected; minimising the public burden for data requested)

### *44. National Plan For Information Systems Protection*

The first version of the Plan largely focuses on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures.

Policy objectives:

- Achieve a critical information systems defence with an initial operating capability by December 2000
- Protect the private information of its citizens that resides on its computers
- Computer Security and Privacy (Ensure public access to data)
- Efficiency (Maximising the use of information collected; minimising the public burden for data requested)

### *45. Cyber Security Information Act*

This Act of 2000 takes into account the vulnerability to external attacks of many information technology computer systems, in order to assist and encourage the secure disclosure and protected exchange of information about cyber-security problems, solutions, tests and results and related matters in connection with critical infrastructure protection.

This act has not been signed by the President of the United States yet.

### *46. Road Map for National Security: Imperative for Change*

This report is a blueprint for reorganising the U.S. national security structure in order to focus that structure's attention on the most important new and serious problems before the nation, and to produce organisational competence capable of addressing those problems creatively.

### *47. Unique Health Identifier for Individuals – A white paper*

This document outlines the policy intent in relation to the rules regarding the requirements for a unique health identifier for individuals, as a part of the process aimed at achieving uniform national health data standards. It seeks to reconcile the need for standardisation and better efficiency on the one hand, with data protection and privacy on the other, and highlights some challenges in this regard.

Policy objectives: The white paper document seeks to outline the issues related to creating standards to support the electronic exchange of a variety of administrative and financial health care transactions and gain comments on the topic from the relevant agencies. It outlines the benefits of a unique identifier and some concerns regarding privacy.

### *48. Uniform Standards for Patient Medical Record Information, report to the Secretary of the US Department of Health and Human Services*

The report describes how the lack of complete and comprehensive Patient Medical Record Information (PMRI) standards has been identified as a major constraint for further development of health system's ability to enhance safeguarding of data, quality and productivity of healthcare delivery.

Policy objectives:

- To advise government how to accelerate the development, adoption, and co-ordination of PMRI standards
- To provide guiding principles for selecting PMRI standards
- To adequately address the issue of confidentiality of PMRI
- To reduce barriers to electronic exchange of PMRI caused by legislative diversity (individual states still differ)
- To provide a framework for co-ordination of the development of PMRI standards within the broader context of national health Information Infrastructure

### *49. National Committee on Vital and Health Statistics Report to Secretary Shalala for the period 1996-1998*

The document is effectively a report to the Executive, the US Secretary of State on the work undertaken in relation to health policy issues. It also contains the relevant policy recommendations in relation to the use (e.g. secondary use for research and administration purposes) and security and confidentiality issues of patients' records.

Policy objective: The main objective is to provide relevant policy recommendations. They could be summarised as follows:

- To insure that confidentiality safeguards are enacted in time an consistent with / parallel to standardisation efforts and reform of healthcare system that is related to e-Health
- To insure further, and achieve a more balanced development in the area of health records (marrying the need to achieve better administrative efficiency and confidentiality).

## *3.2 Policy documents relevant for Trust and Security at European level*

Security is a horizontal topic, rather than a vertical one. It cuts across virtually all the other eEurope policy areas, and it can sometimes be difficult to separate it completely as a stand-alone domain, as security and trust is an enabler for, for instance, electronic commerce or e-Work. However, as such it has been less in the political focus: something that seems to be changing rapidly now. This is not reflected yet in a large number of specific relevant policy documents. The policy documents listed demonstrate a focus on trans-national collaboration for what is recognised to be a cross border (or even more: a border-independent) issue. In some countries more initiatives have been taken already then in others, but relevant initiatives mostly origin from European level. The infrastructure of activities set up in the United States origins from earlier days, based on a concern of national security.

From activities in the field it is clear that a rapid development of appropriate policy action can be expected. Individual concerns about privacy, security and the use of information about their preferences and activities are a barrier to the formation of an effective and broad-based information society. Acknowledging this fact (namely that security and trust are important in the development of the e-economy and the Information Society) eEurope documents state that "the market should, as far as possible, be left to determine the adequate amount of

security for user needs". The focus on Trust and security in the eEurope Action plan is one driver for this, the growing international awareness of the vulnerability of the infrastructure of society goes beyond the eEurope awareness.

According to a recent joint workshop in Brussels, organised by the European Commission and ISPRA bringing together researchers from all over Europe the focus should be on:

1. Complexity, non-linearity, and the prevention, tolerance, removal and prediction of vulnerabilities, interdependencies and failures, considering
   - The design of infrastructures, systems and applications
   - Cost-risks trade-offs
2. Dynamics of technology development and take-up with respect to dependability, trust and risk, considering
   - New technologies (i.e. wireless, mobile)
   - Convergence of technologies and infrastructures
3. Modelling and simulation of interdependencies with the information infrastructure, considering the quantification of dependability, considering
   - Risk perception
   - Technology take-up
   - Evolution of infrastructures

For the short term gaps in understanding should be resolved by bringing together a wide diversity of "circumstantial" information from documents ranging from the EITO yearbook (assessing the relative importance of the risk) to the European Commission reports on Implementation of Telecom liberalisation. But first and for all common definitions need to be found since there is few comparable sources of information available at national level. A series of IST supported projects like Dependability Development Support Initiative have been put in place to support this. For longer term, it is necessary to collect information and data about threats and vulnerabilities from trusted parties.

At a European level, therefore, one can identify the following main issues:

## (I) LEGISLATION ISSUES

### ➢ Human rights

Security and Trust emerge importantly as a "legal issue" at an international level as well as at a national one. An essential document, which, as old as it may be, is still a cornerstone for legislation in the area at both a national and a European level, are the OECD *Guidelines on the Protection of Privacy and Transborder flows of Personal Data*, dated 1980. This document, retrievable on the OECD web site[18], highlights two issues of particular relevance for the Information Society:

1. Privacy
2. International flow of Information

As clearly stated in this document

> *[…] two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.*

[18] http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

Importantly, as referred to also in further documents, "privacy" is considered a fundamental human right, putting the current development of the Information Society in a new light, which allows us to look back (as well as forward) to the foundations of the post-war western society. The *OECD Guidelines* underline that a number of international agreements deal with the issues under discussion, e.g. the European Convention of Human Rights of 4th November 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December 1966).

That "Trust and Security" is (also) about human rights is evident from a larger rose of recent documents, other than the *OECD Guidelines*, but the latter constitute undoubtedly an influential point. One of the European pillars in the protection of data privacy in the 1995 directive is in this field. Notwithstanding its direct impact inside individual EU Member States, this directive has also started to influence non-EU states. A good example of this state of affairs is the *Safe-Harbour Agreement* between the European Union and the United States. The directive clearly states that it is not possible to transfer personal data to third states, unless they apply the same protective and legal standards as those indicated in the directive. The *Safe-harbour agreement* cater for this need in the case of the transfer of data between Europe and the United States. In any case, the overarching concern about data privacy is still the protection of a pivotal human right. This is confirmed in the *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating such persons* (1998), contracted by the Commission of the European Communities, by addressing, for example, the issue of human rights and referring directly to the *European Convention of Human Rights* of 1950, stating that

> *[…] in Europe data protection was construed with particular reference to the right to respect for private life on the one hand and freedom of expression on the other. […] The rooting of data protection in general human rights law - and in particular the relationship between data protection and the rights and interests guaranteed by the European Convention on Human Rights - is of special importance to the Community, since the substantive requirements of the Convention constitute "general principles of Community law", of overriding, constitutional importance within the legal order of the Community (and indeed the Union)*[19].

However, this legal aspect emerging from not only the *Guidelines,* but also the *EU directive on data privacy* and the *Study on the protection of the rights and interests of legal persons*, puts in the spotlight the main issue at stake when considering the topic of "Security and Trust", namely that it operates in a "tension field" between the right to respect for private life and the freedom of information.

Indeed, other documents address this problem, such as the Opinion 5/2001, adopted on May the 17th, 2001 by the Data Protection Working Party. The crucial matter here, for example, is the idea that there should be no friction between privacy and access to information, both to be guaranteed at the highest level. The necessary assessment, is said, should be made case by case, taking into account all circumstances surrounding each particular situation.

> *[…] If the right to public access is found to prevail, public disclosure should be made. If the right to privacy is found to prevail, public disclosure of personal data should be refused*[20].

In all cases, nevertheless, public disclosure of personal data ought to be "fair and lawful".

### ➢ Law enforcement and creation

A second legal issue which emerging from the documentation, and that should co-operate in the fight against e-Crime and in the development if public confidence is the issue of law enforcement.

---

[19] Douwe Korff, Study on the Protection of the Rights and Interests of Legal Persons, Cambridge, October 1998, available at http://europa.eu.int/comm/internal_market/en/dataprot/studies/legalen.pdf

[20] Data Protection Working Party, Opinion 5/2001 On the European Ombudsman Special Report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH, Brussels, 17 May, 2001, p. 6, available at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp44en.pdf

In fact the issue here is the double character of crime over the Internet: on the one hand there are new forms of crime that base their very existence on the new technologies, while, on the other hand, there is traditional crime using the Internet as a new weapon to better reach its objectives. This particular aspect of cyber-crime highlights the issue of law enforcement. While new forms of crime need new specific legislation, in other cases an actual enforcement of existing laws would suffice. Nevertheless, this is not an easy task and requires strong co-ordination among EU Member States. This element has been emphasised during the 1999 Tampere European Council where the head of states and governments of EU Member States have decided to go toward a co-ordinated communitarian approach towards, inter alia, cybercrime. Led by the DG Justice and Home Affairs, these activities have the overarching objective of working towards common procedural and substantive legal measures. More importantly, as concluded during a recent pan-European workshop, the need for closer public and private partnership has been strongly emphasised. This last point leads to the issue of preventive cybercrimes and other Internet-based malicious activities.

In a recent speech concerning *Trust and Security in Electronic Communications: the European contribution*, Erki Likkanen has underlined the importance of prevention of eCrime, stating that this could be possible only where public authorities had the "means to fight back". The Commission's study on "Junk" E-mails of February 2001 (*Unsolicited Commercial Communications and Data Protection*) analyses the difference between the US and Europe on this theme: whereas the phenomenon of "spam" was highly developed in the former, this was not the case in the latter. The document sustains that "spam was addressed in Europe before it ever existed". The main reason the study envisages to explain this distance is that of implementation of existing legislation in Europe, whereas this had not been the case in the US.

> *[…] It was not a question in Europe of drawing up new legislation to deal with a new phenomenon which was not captured by the existing laws. What had to be done was to identify the legal characteristics of spam to determine whether the existing law would have to be amended or extended in order to deal with the phenomenon or whether it would have to be repealed because it was unsuited to the practices employed on the Internet*[21]*.*

Germany offers the most illuminating example since these courts take the view that unsolicited marketing practices (regardless if via the Internet or through other means) constitute unfair competition, and therefore may fall under the Unfair Competition Act of June the 7th 1909.

However, the Information Society and the development of the Internet, cannot be dealt with only through enforcement of existing legislation, but need a specific legislative process as well. Documents such as the *Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures* underline the need of a legal recognition of electronic signatures both, within the EU and towards third states. Such a theme, goes beyond existing legislation, due to the absolute novelty represented by the issue of electronic signatures.

- Borders

A third legal issue of relevance is the borderless aspect of cyber crime (And of general cyber-problems). If, on the one hand, there is a political will, at an EU level, to ensure "free movement of the Information Society", expressed for example in the Directive on Electronic Commerce of June the 8th, 2000, this implies, at the same time, the need for a similar will to fight against crime which may be committed in any place against victims in any place. The OECD Guidelines on Privacy, Security of Information Systems, Cryptography and Consumer Protection in an Electronic Commerce context represent the pivotal point in this context. They all call for international cooperation and creation of an accepted set of rules on information flows.

[21] Serge Gauthronet and Etienne Drouard, Unsolicited Commercial Communications and Data Protection, available at http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf

Similarly, *Opinion 1/2001*, argues for the right of "data subjects" to

> *[…] take action before Courts not only in the jurisdiction of the country where the Data Exporter is established but also in the jurisdiction of the data subject's residence*[22].

Child pornography over the Internet also represents a sort of crime which has developed through the Internet and which has no boundaries. The struggle against this crime, as mentioned in the *Council Decision of 29 May 2000, to combat child pornography on the Internet*, needs international co-operation among Member States as well as between the public sphere and industry. More importantly, though, there is a request for a strong co-operation between states and law enforcement authorities throughout Europe. With specific reference to e-Commerce, for instance, there is a need of coherent EC legislation framework and a European accepted code of conduct. Security problems (for example viruses) are generally acknowledged to be international in nature. The communication from the Commission *Network and Information Security: Proposal for a European Policy Approach* states from the very beginning that

> *There have been some widely reported viruses released onto the Internet causing extensive damage by destroying information and denying access to the network.* Such security problems are not confined to individual countries *but spread quickly across Member States. […]*[23]
>
> *Networks are international . A significant part of today's communication is cross border or transits through third countries (sometimes without the end user being aware of it), so any solution to a security risk needs to take account of this. Most networks are built using commercial products from international vendors. Security products must be compatible with international standards. […]*[24]

while the *Action Plan on Promoting a Safer Use of the Internet*, issued by the European Parliament and the Council of the European Union in 1999, had already declared the need of European co-operation, with respect, nonetheless, for the role of national law enforcement authorities:

> *An effective way to restrict circulation of illegal material is to set up a European network of centres (known as hot-lines) which allow users to report content which they come across in the course of their use of the Internet and which they consider to be illegal. Responsibility for prosecuting and punishing those responsible for illegal content remains with the national law enforcement authorities, while the hot-line aims at revealing the existence of illegal material with a view to restricting its circulation. Differences in national legal systems and culture must also be respected. […]*[25]

The co-operation at EU level should not be limited to political co-operation among states, however, but, as has been said, it should comprise agreements between Public authorities and providers (see the Communication on *eEurope, an Information Society for all*).

---

[22] Data Protection Working Party, Opinion 1/2001, January 26, 2001, p.6, available at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp38en.pdf

[23] Commission of the European Communities, Network and Information Security: Proposal for a European Policy Approach, Communication, 2001, p.3, available at http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_en.pdf

[24] *Ibid*., p. 4

[25] Decision no 276/1999/EC of the European Parliament and of the Council, Action Plan on Promoting a Safer Use of the Internet, 25 January 1999, available at http://europa.eu.int/ISPO/iap/decision/en_print.html

## (II) AWARENESS ISSUES

### ➢ Education

A second issue concerning Security and Trust is that of awareness. This can limit the dangers of cyber crime by preventing it. The communication *eEurope 2002: Impact and priorities* is rather illuminating on this point, and expresses the need of co-operation with Computer Emergencies response teams and improved and stimulated technological development and research at a European level. Various documents (among which one should consider the *eEurope action plan*) emphasise the need of co-operation between different sectors, that is public and private, by an enhanced public stimulation of private initiatives. Education clearly plays an essential role in the creation of public awareness: more than one document states the need of learning processes to adequately use the new technologies.

### ➢ Clarity

Moreover, the definition itself of "data protection", or "cyber security" is often uncertain, or misunderstood, determining a substantial refrain to citizen's awareness. The Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons, states this point unequivocally:

> *There is a lack of clarity, of focus, over the vary nature, aims and objectives of data protection in the Member States which is, not surprisingly, reflected in the international data protection instruments. […] data protection instruments show a similar ambiguity about the nature, objects and aims of data protection. […]*[26]

Awareness may also be weakened by the Website's often obscure or unidentifiable content. This problem emerges in particular in the Action Plan on promoting safer use of the Internet, which underlines the importance of developing filtering and rating systems to make the content easier to identify. But also other documents of relevance to Security and Trust (see for example the already quoted Directive 2000/31/EC) underline this factor, supporting the need of clearer and more identifiable Internet communications –often with reference to commercial communications.

The European Commission has recently started a process of defining its own understanding of specific information security terms. In its Communication *Network and Information Security: Proposal for a European Policy Approach,* definitions of availability, authentication, integrity and confidentiality have been put forward. *Availability* is depicted as the situation where data is accessible and services are operational, despite possible disruptive events such as power supply, natural disasters, accidents or attacks. *Authentication*, instead, is defined as the possibility of asserting the online identity of entities and users. *Integrity* refers to the confirmation of data which has been sent, received, or stored are complete and unchanged. Finally, *confidentiality* indicates the protection of communications and stored data against interception and reading by unauthorised persons.

## *3.3 Policy documents relevant for Trust and Security at national level*

The following chapter will consider four national cases (namely, the UK, Germany, the US and France), highlighting the main issues emerging from the relevant literature.

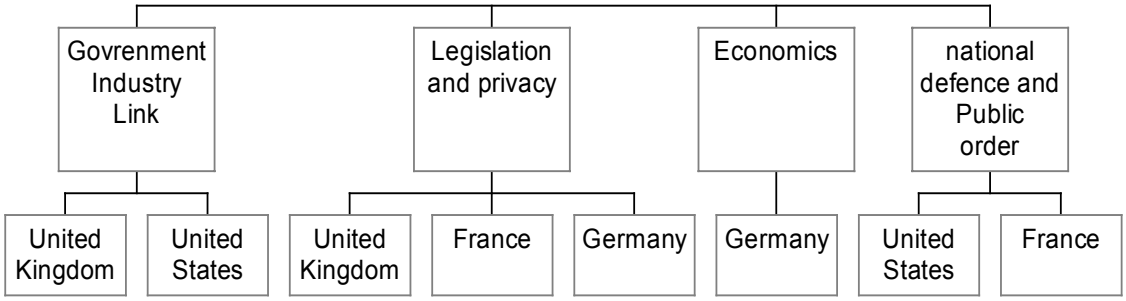
In a broad sense, four essential themes emerge, that is the possible (and, indeed, desired) co-operation between the public and the private sphere, the theme of legislation and privacy, the economic theme and the issue of national defence and public order.

[26] Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons, p.1

However, two points must be preliminarily underlined:

- The above mentioned are the essential trends coming out from the literature, but are not intended to be a conclusive and/or absolute picture. In fact, the developments of the Internet (and of the Information Society at large) are so fast that a complete and unbreakable image is not possible. It should suffice to recall the definition of "Internet year" as suggested in the US *National Plan for Information Systems Protection* of January the 8th, 2000 - "…a term commonly used to mean three calendar months"[27].
- The issues are relevant for all the countries considered. However, a distinction has been operated among them according to the weight given by different states to different issues. One can then find that national security is mostly a concern of the United States and of France, while the focus on human rights (not certainly absent anywhere) is of particular interest in the Federal Republic of Germany.

The graph below summarises these points.




### 3.3.1 United Kingdom

The documentation relative to the UK highlights the following issues:

## (I) GOVERNMENT AND INDUSTRY LINK

This Issue emerges in more that one document relative to the United Kingdom. In particular, the consultation document *Promoting Electronic Commerce*, presented to Parliament by the Secretary of State for trade and Industry on July 23, 1999, with reference to the problem of "spam" (mentioned above), took the position that Industry should

> *[…] take effective voluntary measures, but […] the Government should keep a watching brief and be ready to take legislative action if necessary […]*[28]

The necessity of such connection between public and private, is linked to the increased dependence on IT, world wide and in the UK specifically. The *UK ITSEC evaluation and certification,* which is run by the government body Computer and Security Evaluation Group (CESG), underlines the fact that this trend enhances also the potential risks, such as those associated with unauthorised access, which can be fought only by increased IT security. In the view of the *Scheme* "IT security" means confidentiality, integrity and availability of information, factors which develop confidence by the public. This aspect has also been confirmed by the Information Assurance Advisory Council (IAAC), a non-profit independent organisations which reunites leading UK public and private companies to discuss these topics. In their 2000 Annual Symposium, all the speakers have clearly emphasised the risks

[27] National Plan for Information Systems Protection , January 2000
[28] UK Government, Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report, Promoting Electronic Commerce, 1999

and threats association by the strong inter-action between the public and private information and networks infrastructures. Consequently, a stronger partnership between public and private organisation is required or, even, necessary to shun off the dangers of malicious activities and general hardware/software faults.

## (II) LEGISLATION ISSUES

The Electronic Communications Bill highlights mainly the issue of law enforcement as necessarily accompanying the legislative process which should renovate the legal corpus on the basis of the new needs emerging from the Information Society and the new information flow. The power to modify legislation is explicitly mentioned in the Bill, where it states:

> *[…] the appropriate Minister may by order made by statutory instrument modify the provisions of any enactment or subordinate legislation in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) […]*[29]

On the other hand, law enforcement is a basic means of combating cyber-crime as well. The United Kingdom has been one of the first countries to have developed specific legislation concerning specific forms of cybercrime: the 1990 *Computer Security Misuse Act*. Nevertheless, as indicated by several prosecution cases involving computer crimes, the issue of enforcing the provisions of this law, as well as of other computer and Internet-related criminal legislative measures, present many practical and operational difficulties. This last point has been confirmed by the explanatory notes of the *Electronic Communications Bill*, contained in the consultation document presented to the British parliament in July 1999 *Promoting Electronic Commerce* refer to this issue underlining the possibility (and indeed the necessity) of enforcing as much as possible existing legislation when the use of new technologies appears to be the instrument of traditional forms of crime.

Clearly, then, as emerges from supranational documents referred to in the previous section, law enforcement is one side of the coin, the other being the legislative process necessary to link legal commitments to both the new potentialities and the new forms of criminality intrinsic in the Information Society's development. Therefore, the above mentioned document *Promoting Electronic Commerce*, next to the need of law enforcement, regards also as essential the updating of procedures and the possibility of removal of restrictions which prevent the use of electronic communication.

The recognition of this double character of Security and Trust within the Information Society (the "tension field" between information and privacy), is a cornerstone of the UK's policy in the field. In fact this country played a leading role in the debate. Nevertheless, it was only after continuous interaction between the public and private sector, that the UK government appreciated the need to deal with both authentication and confidentiality issues in a single framework.

Moreover, as emerges also from the supranational documents, the borderless aspect of the Information Society is also a concern for the UK. If, on the one hand, this characteristic opens new doors, on the other, not only it offers new opportunities for criminal offences, but complicates the task of security evaluation. The only way to compare results of different evaluations, world wide, seems then to be international mutual recognition of security systems and evaluations based on impartiality, objectivity, repeatability, reproducibility. Together with France, Germany, the United States and the Netherlands, the United Kingdom has been a leading force in drafting and devising an international standard for the evaluation and certification of the security functionalities of product and system, the Common Criteria. Through this international standard, it is possible for companies to have their products evaluated and certified in one country knowing that the results of this process will be immediately recognised in other countries.

[29] UK Government, Electronic Communication Bill, available at http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmbills/004/2000004.htm

The United Kingdom has also been instrumental in turning one of its national standards, BS 7799 for Information Security Management, into an international one through the process provided by the International Office of Standardisation (ISO). Drafted at the beginning of the 1990s, this UK standard has been the result of a strong co-operation among government departments, in particular the Department of Trade and Industry (DTI), and private companies such as Marks and Spencer, British Airways and many others. Soon after its release, a formal independent evaluation and certification scheme has been created, which was rapidly reproduced in other European and third states such as Australia and New Zealand. However, due to the borderless nature of information and network infrastructures, the UK has soon appreciated the need to devise a global response for information security management. This led to a global effort to make BS7799 an international standard.

### 3.3.2 Federal Republic Of Germany

The documentation relative to Germany highlights the following issues:

## (I) LEGISLATION ISSUE

- Human rights

The use of the Internet can hide the risk of unlawful disrespect for human rights and dignity, not only in terms of privacy as a central human right to be preserved, but also with respect to materials (violent pornography, written materials inciting xenophobia or racism etc.) which see the Internet as a new and relatively smooth means of distribution. German policy-makers are aware of this problem, as emerges from the documentation. For example, the Action Programme *Innovation and Jobs in the Information Society of the 21st Century* states that

> *Protecting human dignity during use of the Internet and in view of its rapid spread is a central political and a general social task*[30]*.*

Within this aspect, the international/borderless character is apparent: not only the new information technologies have no frontiers, but human dignity in itself is "global" in nature. Therefore, there is a call for trans-border co-operation in this respect as well. Indeed, *Innovation and Jobs* affirms that, considering the global nature of the new media, national regulations can have only a limited effect. Therefore there is an urgent need for them to be flanked with European and international agreements.

Being privacy a central human right, implies that data protection must be guaranteed. But the *Law on Electronic Signatures*, in particular, fits together two different but compatible rights: that of the applicant of a qualified certificate, and that of the provider. The former has the right to privacy and not to see his data given in public domain, but, at the same time, the certification-service provider have the right to reliably identify persons who apply for a qualified certificate.

- International co-operation

Also German documents acknowledge the intrinsically borderless character of the Information Society. The *Law on Electronic Signatures* affirms the need not only of co-operation with authorities, but also the necessity of international mutual recognition of foreign qualified certificates, provided they are in line with EU legislation:

> *Electronic signatures for which a foreign qualified certificate has been issued by another Member State of the European Union or signatory to the treaty on the European Economic Area shall be equivalent of qualified electronic signatures if they correspond to Article 5(1) of Directive 1999/93 EC of the European Parliament and of the Council of 13 December 1999 on a*

[30] German Government, Innovation and Jobs in the Information Society of the 21st Century, 1999, available at http://www.bmwi.de/Homepage/English%20pages/Publications/Publications.jsp

> *Community framework for electronic signatures (OJ EC 2000 No. L 13, p.2) in the current version*[31].

Also Innovation and jobs in the Information Society of the 21st Century, underlines the issue of the borderless character of Security and Trust, reminding that, due to the global character of the networks, "…data protection is an international task1".

The Information and Communication Services Act. by its part, already raised the issue in 1997 when dealing with digital signatures (see art. 3, § 15).

Finally, as stated above, when the question of human rights is at stake, again the international co-operation is needed with utmost vigour.

- Enforcement and creation of law

In Germany the issue of legislation enforcement vs creation of new laws emerges with strength. In *Innovation and Jobs in the Information Society of the 21st Century* this issue comes out. In particular there is a request for reliable conditions not only with reference to security for consumers, but also in other areas such as taxation of Internet transactions and labour and social law. Germany wants, therefore, to avoid any legal fragmentation. At the same time the necessity to issue new sorts of law is explicitly mentioned, with reference to the developments in modern information and communications technologies. "The formal requirements of civil law, it is claimed,

> *are no longer adequate to modern legal business. The need for written documents is often preventing rapid action using modern technology*[32].

Similarly, the *Trusted eCommerce* report by TeleTrusT Deutschland e.v. also envisages the need of an amendment of previous legislation in order to update it to the trust and security needs in the new Information era.

## (II) ECONOMIC ISSUE

Data Security and the fight against cyber-abuse is not only a legal matter, as important as it may be, but, as German documentation tends to underline, it is also a question of economic advantage. In particular, it is said, competition can be severely damaged by cyber-abuse and the distrust this may cause in the public towards the developments of the Information Society. For example, the above mentioned Action programme *Innovation and jobs in the Information Society of the 21st Century* affirms this clearly :

> *[…] ensuring efficient data protection is also an important competition factor for the suppliers of these services*[33].

At the same time, security for users enhances confidence. This is an essential foundation for the development of eCommerce itself and the bettering of competition. German documentation shows the direct link between these two factors (that is IT security and economic advantage). The quality of security provided forms a major part of competitive advantage, according to the quoted *Innovation and Jobs*. Thus the German government intends to engage itself in the development of IT security for German IT products and services.

Finally, the documentation highlights the rights of all citizens, other than consumers alone: also personal data of any employee must be object of protection, although s/he is not a "customer" in that specific circumstance. The point here is the fact that privacy is, as reminded in European documents, a fundamental human right which, therefore, goes beyond the qualification of an individual being a consumer/customer rather than fitting in a different category. At the same time there is an inevitable need to ensure also the right of the employer to be informed. What is claimed for is confidence for all parts involved. Fitting together these different necessities is the task and the challenge the German government has set itself.

---

31 German Government, Law on Electronic Signatures, 1997
32 Innovation and Jobs, p. 39
33 Ibid.

### 3.3.3 United States Of America

The three basic issues arising from US documents are those of national defence, privacy and the link which should create itself between the sphere of government and that of the private sector.

## (I) NATIONAL DEFENCE

- Defence of critical infrastructures

A main issue emerging from the US documents is that of national defence. In fact, information security has become a pivotal national defence priority in the US and, therefore, is having a significant impact on the direction of several legislative processes. This is becoming evident in the US efforts to protect their so-called critical infrastructures. The *Computer Security Act* of 1987, has taken away from the National Security Agency (NSA) the responsibility for the security of the US Federal information and network systems. This task was passed to the National Institute for Standards and Technology (NIST). It has also called for the establishment of a Computer Security and Privacy Board, hosted by NIST, which has been chaired up to last year by Dr Willis Ware of Rand Corporation, Santa Monica.

The *Presidential Decision Directive NSC-63* defines critical infrastructures as

> *those physical and cyber-based systems essential to the minimum operations of the economy and government*[34].

In fact, the question arises due to the grand military and economic strength of this country. The Phase III report by U.S. commission of national security/21st Century *Road Map for National Security: Imperative for Change* (February 2001), states explicitly that the United States' strength, not only

> *[…] does not render it immune from these dangers. To the contrary, U.S. preeminence makes the American homeland more appealing as a target, while America's openness and freedoms make it more vulnerable*[35].

Thus, on the one hand, military power could induce enemies (present and future) to harm the US in "non-traditional ways". On the other hand, because of the increased reliance of the United States' economy upon interdependent and cyber-supported infrastructures, "non traditional" attacks may be capable of significantly harming the their safety.

The *National Plan for Information Systems Protection*, of the beginning of 2000, flows directly from *PDD 63*, and therefore considers with particular devotion the matters surrounding defence and national security.

Some quotes may suffice to spotlight the relevance granted to this issue by the above mentioned *National Plan*:

> *[…] hostile powers and terrorists can now turn a laptop computer into a potent weapon capable of doing enormous damage If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack. […]*
>
> *[…] In the next war, the target could be America's infrastructure and the new weapon could be a computer-generated attack on our critical networks and systems. We know other governments are developing that capability. […]*

[34] USA Presidential Directive 63, 1998

[35] US Government, Road Map for National Security: Imperative for Change, February 2001, available at www.nssg.gov/PhaseIIIFR.pdf

> *[…] We know of foreign governments creating offensive attack capabilities against America's cyber networks. […] The threat is that in a future crisis a criminal cartel, terrorist group, or hostile nation will seek to inflict economic damage, disruption and death, and degradation of our defence response by attacking those critical networks. Director of Central Intelligence George Tenet testified to Congress: "This threat is very real." […]*[36]

- Education and training

Given the role of national defence as issue at a US level, the question may arise on how to assure it (as far as possible). Inevitably linked to that issue, therefore, is the one of education/training, also profoundly taken into account by US policy makers. Considered the high degree of dependence on critical IT infrastructures, a consequence is the necessity of educating persons to be able to operate within this new and fast-changing environment, in view of defence against innovative forms of crime (cyber-crime).
Since the beginning of the 1980s, the US federal government called for training schemes to enhance awareness of all employees in the Federal Agencies.

But, once again, the *National Plan for Information Systems Protection* takes this issue in greater consideration. Here the need of educating a corps of young computer scientists "…to help defend our federal cyber systems…" is explicitly stated in the introductory message by former president Bill Clinton., while the plan, in its third program, claims that there is a requirement of new skills in this ambit. Finally, program 7 of the same *Plan* ("Train and Employ Adequate Numbers of Information Security Specialists") addresses the same issue, and research in the field shall be publicly funded and sustained.

It is noteworthy, however, that such educational effort, is manly directed to national security, one of the main aims of the US policies in the field of Information Society. The report *Road Map for National Security: Imperative for Change*, for example, referring to education, says:

> *This is not a matter merely of national pride or international image. It is an issue of fundamental importance to national security*[37]*.*

This approach is also confirmed by several out-reach activities carried by organisations such as the National Security Agency or the Defence Advanced Research Programme Agency (DARPA).

Nevertheless, in January 2000, the US federal governments has also launched a series of activities aimed at enhancing information security education and awareness. It has launched the Federal Cyber-services Training and Education Initiative to make sure that there is an adequate supply of high skilled Federal information systems security specialists. One of the cornerstone of this programme is the programme *Scholarship for Service*. Students are sponsored towards information security degrees in exchange of a set time of employment period in one of several federal or national department and agency. In order to support this programme, the US federal government has also launched a programme aimed at establishing Centres for Information Technology Excellence.

These are a set of selected academic institutions that are to provide high-calibre, cutting edge information security training and certification of current Federal Information Technology employees, federal contractors, and Federal Cyber Services candidate. The US Federal government is also working in raising information security awareness among young people through the *High School Awareness and Outreach Programme* and *Academy of Information Technology*. These programmes are to provide secondary high-schools with the opportunities to partner with community colleges, universities and businesses in order to prepare students for careers in information technology fields.

---

[36] PDD 63
[37] Road Map for National Security: Imperative for Change

### (II) PRIVACY

Privacy is acknowledged also at a US level, as an issue to take into consideration. The *National Plan*, for instance, devotes to this matter a separate paragraph, entitled "Protecting Privacy and Civil Rights". In this context, however, the issue emerges more as a interrogative on the possible trade-off between privacy and infrastructure assurance objectives. This is stated explicitly:

> *[…] portions of the Plan may give rise to concerns that personal privacy rights may be sacrificed in exchange for infrastructure assurance objectives*[38].

The question here is how to maximise both aims (privacy and assurance).

### (III) GOVERNMENT AND INDUSTRY LINK

Also in the United States of America, the issue of public/private sector relations emerges. All documentation spotlights this point with particular vigour: The *PDD 63* as well as the *National Plan* or the *Cyber Security Information Act* all underline the inevitability of such a link if cyber-security has in order to pass from the "want" dimension to the "factual" dimension. For example the *Cyber Security Information Act* underlines how, among others, its purpose is also

> *[…] to assist private industry and government in effectively and rapidly responding to cyber security problems*[39]

While the *PDD 63* devotes a specific paragraph to the issue ("A Public-Private Partnership to Reduce Vulnerability"), this is recalled more often throughout the *National Plan*, claiming the need of a partnership "unlike any we have seen before"[40].

## 3.3.4 Republic Of France

### (I) NATIONAL DEFENCE

In France, similarly to the US, a central part of the debate relates to the issue of national defence, with an extra focus on internal public order. The general secretary of National defence has at its disposal the so called "Service central de la sécurité des systèmes d'information (SCSSI)", which is of assistance in the exercise of its missions.

On the one hand, the issue of national defence against foreign possible cyber-attacks emerges with strength, on the other, also internal public order is a central issue. These issues, of central importance for France, led, in 1995, to the compilation of an important directive (*Directive n. 4201/SG*), which still represents an important milestone in French policies on security and trust.

On national defence the *Directive 4201/SG* explicitly states:

> *Pour assurer à l'information le degré de sécurité voulu il faut donc protéger les systèmes utilisés contre les manœuvres captatoires ou les intrusions susceptibles de la trahir, de l'altérer ou de la détruire. Ceci est particulièrement nécessaire lorsque la sécurité de l'Etat ou les intérêts fondamentaux de la nation sont en jeu. C'est ainsi que les systèmes d'information gouvernementaux, c'est à dire les systèmes d'information qui*

[38] USA Government, National Plan for Information System Protection, 1999 p.3, available at http://www.piersystem.com/clients/PIERdemo/ACF870.pdf

[39] US government, Cyber Security Information Act, available at http://www.ombwatch.org/info/2000/HR4246.html

[40] President's Message, in *National Plan*

> *gèrent les informations classifiées de l'Etat (défense. diplomatie, sécurité de l'Etat), doivent jouir de la plus haute protection. […]*[41]
>
> *Sécuriser l'information doit être un souci général. Sécuriser les systèmes d'information est une obligation nationale majeure.*[42]

The same Directive also states clearly the importance of public order, when asserting that satisfying private requests is a national duty, bearing in mind, however, that the security of the state and public order must be ensured.

Also the *Projet de loi sur la société de l'information* (of year 2001) underlines the role of national defence.

**(II) LEGISLATION ISSUES**

A second issue is that of legislation.
Also in France there is a debate on whether there should be new legislation to avoid breaches, or whether the enforcement of previous legislation might suffice. Not surprisingly, similarly to the cases of the UK, Germany and the US, a coexistence is required.

The *Projet de loi sur la société de l'information* suggests a stronger enforcement of existing legislation, but also modifies substantially previous laws, especially with reference to cryptology and e-commerce. The latter, it is said, sees confidence as its very foundation, without which it cannot survive.

The *Note du Service Central de la sécurité des Systèmes d'Information au sujet de la protection des informations et systèmes sensibles dans les administrations* of May the 2nd, 2000, underlines the importance of confidentiality and integrity of information as a means to obtain security (and therefore trust). Disrespect of such issues would be a major threat to private life, considered, as is known, a fundamental right. And one must bear in mind the importance given to fundamental rights in France. The frequent reference to the *Declaration of the rights of man and of the citizen* of August 26, 1789 is, therefore, not incidental[43], demonstrating again how themes of trust and security can often fit in general and timeless values.

The following extract of the *Declaration* is, quite clearly, significant also with reference to the information society and the issues of security and trust

> *The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law*[44]*.*

## *3.4 Relevance for SIBIS*

Statistics on Trust and Security are hardly available, other then use of hardware and penetration of Information Society services. In particular reporting on issues such as cyber attacks and hacking are non existent, or anecdotic, since most (private) organisations are not

[41] Directive n. 4201/SG *Sécurité des systèmes d'information*, 1995. "To assure information the desired level of security it is, therefore, necessary to protect the used systems against intrusions which could betray, alter or damage it. This is particularly necessary whenever security matters or national interests are at stake. It is in these contexts that governmental systems of information- these systems generating information classified as "of the state" (defence, diplomacy and security of the state), must enjoy the highest elvel of protection".

[42] Directive n. 4201/SG *Sécurité des systèmes d'information*, 1995. Ensuring information should be a general concern. Ensuring information systems is a greater national obligation.

[43] See for example the *Compte-rendu de la table ronde sur la cybercriminlité du 2 décembre 1999*, or various comments on French legislation

[44] *Declaration of the Rights of Man and of the Citizen*, Paris, August 26, 1789, article 11

inclined to share this information, considering it as a potential commercial threat. This creates serious problems in terms of validation of any useful data openly available. It is possible to split sources of data into 3 main groups: industry, consumers and public sector. Consumers do not mind revealing to others that they have been the victims of cybercrime or related Internet malicious activities. For industry this is a significant concern to such a point that most of the data available is anecdotal evidence and quantitative data regarding virus intrusions. Differently, the public sector is stipulated (or should be) by regulation to provide data and information about intrusions. An interesting example of this state of affairs is the UK UNIRAS system, which collects data of intrusions or malicious activities against British government departments.

Efforts should concentrate on three specific indicators, which can be a combination of available traditional and innovative measures. These refer to

- On-line malicious activities
- prevention of on-line malicious activities and downtime
- On-line interactions facilitators[45]

Many indicators presented in the current report address some aspects of these categories. However, their major failure resides on the fact that they often do not differentiate between industry, consumers and public sector, although the political literature underlines the importance of such differentiation.

Without good performance indicators, firms, security suppliers and consumers are constrained from making informed decisions about the current or desired level of security and privacy. This goes both for the United States and Europe.

However, in the United States these issues are now approached by installation of so called ISAC offices: clearing houses per branches that are independent, in which information from branch industry organisations on intrusions is recorded and reported to government in such a way that it is not traceable to individual organisations. In this way cyber attacks will be detected faster, and government in co-operation with industry can take appropriate measures. The ISACs are only recently in place, and still have to become more effective, which will take time and compromises from both industry and government.

In Europe the problem is slightly different. Although private industry is hesitant to share information with anyone, including public authorities, the mistrust is not as deep as the relations in the United States between private industry and government. However, in addition to the hesitance to share information about “weak spots” in the company, the expected results of appropriate government actions are low because of lack of knowledge, means and manpower (although varying per Member State).

Establishing such “centres” in Europe would allow getting better statistics representing the level of security as related to threats. New joint research activities need to support the development of new policy in this area. This research needs to consider the different infrastructures, the different application domains and their interdependencies with the Information Infrastructure. This shall cover the entire life cycle from design up to evaluation, and from deployment to operations and maintenance.

However, the policy documents allow us to score activities relevant to Trust and Security on process lines. In this respect three categories seem relevant.

- <u>Strategy development.</u>

This category could include the following elements:

[45] Online trust and confidence does not involve exclusively issues related to information security, cybercrime and downtime. Especially in a business-to-consumer environment, individuals associate trust towards electronic commerce shops that offers effective solutions or avenues to tackle problems such as redress, out-of-court settlement, data privacy protection, delivery, customer support (for example seals and Web-based certificates)

- Development of public-private partnership
- Development of strategy documents and implementation plans.
- Foresight of common standards, with relevance to the issues raised.
- Funding of security initiatives.
- Organisation of the initiatives ( e.g. national vs. supranational)
- Required legislative changes, harmonisation etc.
- Timeline for implementation.

➢ Implementation

Have necessary law and regulation changes been made?

➢ Evaluation

This category could include the following elements:

- Mechanisms put in place for collecting regular monitoring information
- Procedures developed by the government for evaluation of cyber-crime and defence against it.

The outcome of ICT initiatives on security and trust can also be measured. Such measures may include the following four:

- Effectiveness of public-private co-operation
- Impact of the relevant initiatives on the actual defeat of cyber-crime
- Impact of the relevant initiatives on the enhancement of public awareness
- Trade-off between cyber-crime and economic development

# 4 Summary of current issues and way forward

Security and Trust are likely to become increasingly key factors in the development of the Information Society in Europe. In fact, a number of issues have emerged from the analysis of policy and statistical documents at a European as well as a national level. These range from legislation matters to economical ones, from relations between public and private bodies within a nation to international co-operation in the struggle against unlawful behaviour related to the Internet's developments. Last but not least, the US (and France) express a particular concern about national security, which is becoming increasingly important in Europe as well.

The goal is then to draw attention to the essential issues emerging from the previous sections, to summarise what indicators currently exist and, finally, to highlight new concerns and unanswered questions following from the gaps in the literature in order to initiate a process of indicator building to fill such gaps.

The previously quoted Communication of the European Commission, *Network and Information security,* suggests with reference to Information Society developments that a distinction should be drawn between two general issues: the increasing possibility for criminal activitiesbased by ICT and new technological developments . This remark is consistent with our findings as, within these basic categories, it is possible to fit the main issues which have emerged from the literature.

As the graph below shows, three "sub-issues" fit into the domain "Increased potential danger" deriving from the Information Society developments. These are linked to national defence, economics and relations between public and private bodies.

If, on the one hand co-operation at an international level seems a necessity to combat economically disruptive actions, on the other hand a strong agreement between the public (governmental) and the private (industrial) sector is also unavoidable[46]. Finally, documents relevant to the USA show strong evidence for the case of critical infrastructure protection and education and training[47], in order to assure national defence.

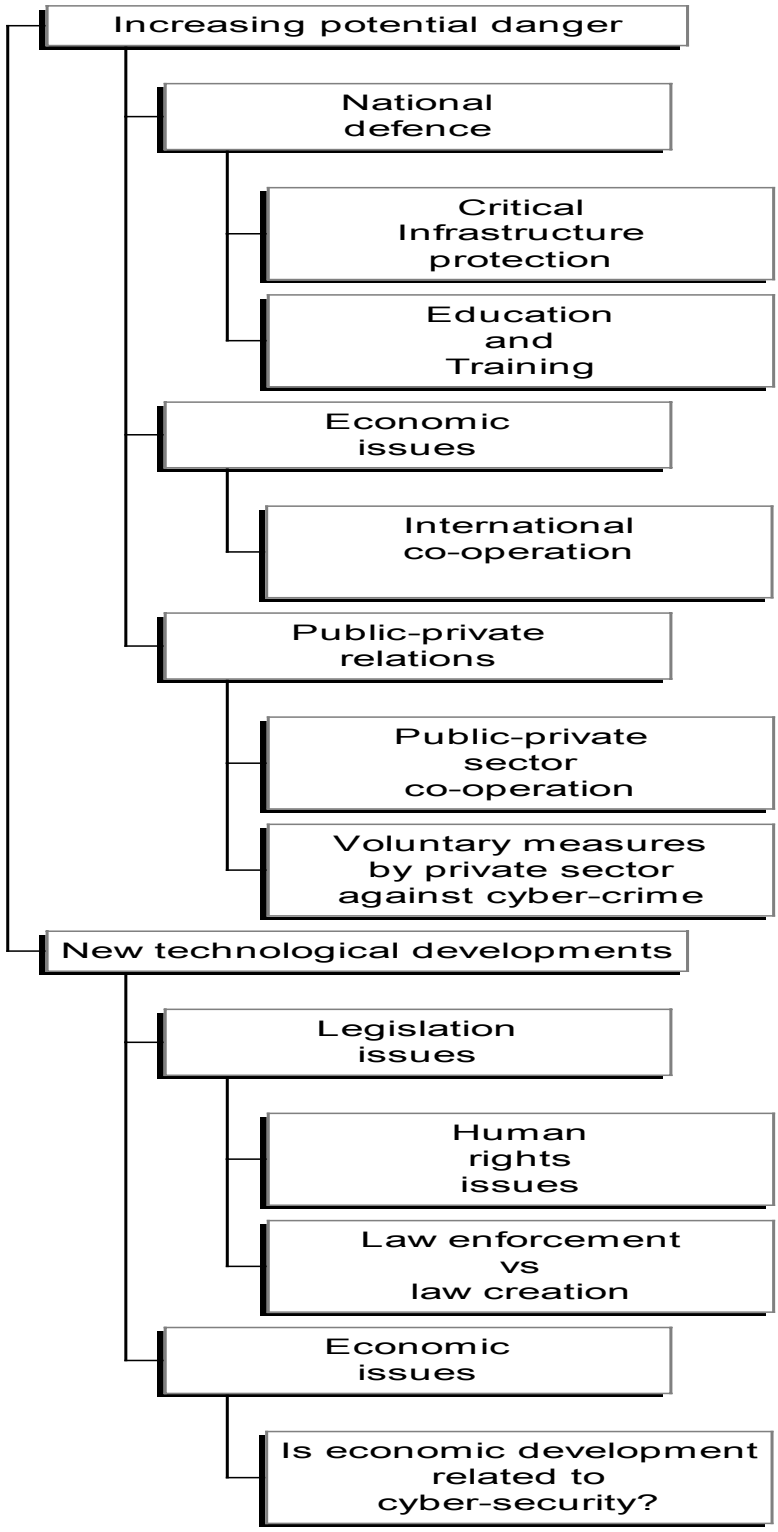
The new technological developments also face new challenges, both at a legislative level (such as the defence of privacy- as a human right- and the issue of law enforcement vs creation of new law) and at an economic level (German documents underline the possible relation between economic development and cyber-security[48]).

[46] See Ch. 3.3, with reference to the UK and USA

[47] See for example *Computer Security Act* (1987), PDD 63, *Road Map for National Security: Imperative for Change* (February 2001),

[48] See *Innovation and jobs in the Information Society of the 21st Century*, quoted in Ch. 3.3, with reference to the Federal Republic of Germany.

Given these issues, the question which arises, and that has most relevance for the SIBIS project, is one regarding the set of indicators currently available on this topic and possible future ones.




The tables below are a first attempt to address the matter with relevance to increased potential danger and the new technological developments.

# INCREASING POTENTIAL DANGER

| ISSUE | INDICATORS | WAY FORWARD |
|---|---|---|
| **Economic matters** | | To what extent can we link economic co-operation to international co-operation against cyber abuses? How valid (if at all) is the following relation?:<br>*int, cyber coop. = f(int. econ. coop)* |
| **Public-private relations** | | The issue here is twofold:<br>How can the co-operation between government and private sector be measured and assessed?<br>Is the private sector taking steps to adopt voluntary measures against cyber attack?<br>An indicator could be, then, the % of private firms adopting voluntary measures against cyber abuses. |
| **National defence** | Knowledge of information logged per page is the only (innovative) indicator presented by GVU in 1998. It can give an idea of the level of cyber education and awareness. | % of Universities/schools offering compulsory computer courses<br>How many of such courses deal directly with cyber security issues?<br>Number of cyber attacks<br>Does the development of the Information Society enhance (or lower or none) citizens' perception of their country's strength (or vulnerability)? Does it enhance (or lower, or none) the perception of a country's strength (or vulnerability) by other states? Is it possible to see if it lowers or enhances a nation's strength in fact?<br>perception of national strength = f(ΔIS)<br>National strength = f(ΔIS) |

# NEW TECHNOLOGICAL DEVELOPMENTS

| ISSUES | INDICATORS | WAY FORWARD |
|---|---|---|
| **Legislation** | Financial losses and problems encountered. This does not say much about law enforcement and new legislative efforts.<br>Some innovative indicators (GVU, 1998) dealing with citizens' perception of security and privacy (% of persons accepting the possibility of being listed in- hypothesised E-mail directory)<br>Levels of international criminal activity with reference to computer related crime. | Impact of convenience as opposed to privacy on the awareness of cyber-crime and its element of human rights violation. What relation is there between the importance given to convenience (innovative GVU indicator) and the number of complaints?<br>*complaints = f(trade-off privacy/convenience)*<br>Impact of relevant initiatives on awareness and actual defeat of cyber crime. (Relevant initiatives include legislative initiatives).<br>Indicators investigating the relation between changes in legislation and variations of different factors, such as cyber crime complaints (awareness), security features adopted by users, computer security spending, preference for on-line vs off-line shopping etc.<br>*Δcomplaints = f (Δleg)*<br>*Δsecurity features adopted = f (Δleg)*<br>*Δsecurity spending = f (Δleg)*<br>*Δonline shoppimg= f(Δleg)* |
| **Economics** | | Relation between cyber problems and confidence, which, therefore, influences competition.<br>*competition = f(cyber confidence) = f(-cyber problems)*<br>Is there a trade-off between cyber crime and economic development? If yes, how strong is it and what is the relation between actions of international co-operation for economic development and actions of international co-operation against cyber crime (and for cyber security?) To what extent do states co-operating economically co-operate also for cyber security?<br>*Δeconomic development = f(-Δ cyber crime)* |

These issues suggest the need for a methodology defining standardised indicators to measure trust, confidence and security in the context of the information society. The following sections shall address the matter by arguing for the need to move away from seeking a single benchmark metric for trust, confidence and securityand concentrating instead on defining three distinct indicators for security.

As a basis for indicator development, **security** is defined as *the combination of technical and managerial processes that aim to foster confidentiality, privacy, integrity & availability of data and information systems, as well as to provide authentication and non-repudiation functionalities*.

The analysis then concentrates on the identification of the **units of analysis**, which should guide data collection based on surveys and existing indicators. Finally, the report examines the three single indicators that should be used as the security benchmark:

- Online Malicious Activities
- Prevention of Malicious Activities and Downtime
- Online Interaction Facilitators

Particular attention is given to identifying possible approaches for combining traditional and innovative indicators in order to derive a single aggregate measure. However, the report concludes by arguing that the three indicators should be kept separate. The reason is that they cannot be homogenised or compared unless they are quantified using a common base.

# 5 Discarding Trust as a Statistical Indicator for the Information Society

European policy on the Information Society is often framed in terms of promoting “trust and confidence” but defining trust is very difficult. According to the US National Research Council, a system is defined as *trustworthy* when it performs as expected despite environmental disruption, human user and operator errors and attacks by hostile parties. Trustworthiness encompasses the following attributes: "correctness, reliability (conventionally including secrecy, confidentiality, integrity and availability), privacy, safety, and survivability".[49]

The information security literature characterises “trust” as a particular functionality provided by public key infrastructures (PKI). PKI solutions allow two or more actors to authenticate one other and, more importantly, to establish a situation where neither party can repudiate commitments undertaken electronically.

In the more general context of the information society and electronic commerce, trust refers to a combination of subjective and objective elements, which are only marginally related to information security. They refer more to “soft” issues about on-line marketing, quality control, business process and customer relation management. [50]

According to the literature on marketing relationship, trust can be conceived of as the situation where one party has confidence in the reliability and integrity of its exchange partners. Several scholars characterise trust as the willingness of an individual or organisation to rely on an exchange partner in whom one has confidence. [51] Others view trust as an “order

[49] National Research Council, Trust in Cyberspace, (Washington, DC, USA: National Academy Press, 1999) p.14

[50] An exception to this state of affairs is represented by the report Trust in Cyberspace by the Computer Science and Telecommunications Board of the US National Research Council. Its approach nevertheless, is directed primarily to assess those factors that might lead to software and hardware failures and, at the same time, to identify public policy responses. The objective of this project was not to measure trust. See National Research Council, Trust in Cyberspace, (Washington, DC: National Academic Press, 1999).

[51] See John Butler, “Towards Understanding and Measuring Conditions of Trust: An Inventory”, The Journal of Management, vol.17 no.4 (April 1991), pp.743-663, Robert Morgan and Shelby Hunt, “The Commitment-Trust

qualifier", which is the belief or expectation that the word or promise by a merchant can be relied upon and the seller will not take advantage of the consumers' vulnerability. In this context, trust does not stem from technical arrangements but arises from a complex mix of legal, social, cultural and individual factors. These factors are complex to quantify, especially in an Internet or information society environment. As argued by Sirkka Jarvenpaa and Noam Tractinsky, "in Internet commerce, merchants depend on an impersonal electronic storefront to act on their behalf". Therefore, the main issue to be examined is to assess how trust is established in online environments.

Sapient, a leading global e-commerce consultancy firm, has attempted to provide an answer to assessing trust formation. Sapient suggests that trust towards electronic commerce involves the following components:

- **Seals of approval**: these are symbols informing users that a certain level of security has been ensured
- **Brand and Fulfilment**: this is mostly the result of the promise to deliver specific attributes; credibility is the result of users' previous experiences.
- **Navigation, Presentation and Technology**: this refers to the ability of users to use a particular Internet-based activity and involves the use of technological solutions that suggest quality and professionalism.[52]

A larger set of trust-promoting elements was identified through a survey of UK Internet users and shoppers conducted in 2000 by the National Consumer Council. The project concluded that users have difficulty in trusting electronic commerce operations not only because of concerns about the security of their data and information, but also as a result of the lack of national and international regulations and difficulty in assessing merchant reputation. The report concluded that, although consumers' confidence in the new medium may grow as they build up their experience and expertise, some of them "see no prospect of ever shopping online, either because they feel it is not attractive enough, or they see no prospect of gaining online access; others recognise that the Internet and online shopping have limitations". [53]

Similar conclusions were reached in a survey conducted by Consumer International.[54] Notwithstanding some improvements since 1999, the CI data indicated that Internet users still have not developed a strong sense of trust towards electronic commerce due to a combination of factors. First, individuals expressed concerns about being provided with full data and information on the cost of transactions initiated through electronic means but completed through physical processes. For example, there were concerns about the fact that the prices indicated on e-commerce sites are sometimes different from the actual final charges, or that goods ordered through the Internet are sometimes not delivered. A second major apprehension relates to concerns about the global nature of the Internet. Users do not know where a site with which they are interacting is based. Finally, users are confused about the overall terms and conditions of electronic transactions. [55]

These concerns are also expressed in relation to e-government initiatives. In September 2000, the Information Technology Association of America released a survey, suggesting that over 60% of respondents were less likely to interact with government institutions due to security fears, as well as due to a lack of reliable information and data about the service and their transactions.[56]

---

Theory of Relationship Marketing", The Journal of Marketing, vol. 58 no.3 (July-September 1994), pp.23-34a and Donna Hoffman, Thomas Novak and Marcos Peralta, "Building Consumer Trust Online", Communications of the ACM, vol42 no.2 (April 1999), pp.81-84

52 Cheskin Research and Studio Archetype/Sapient, E-Commerce Trust Study, available at http://www.studioarchetype.com/cheskin/

53 National Consumer Council, E-Commerce and Consumer Protection, August 2000

54 CI is the federation of consumers' organisations dedicated to the protection and promotion of consumers' interests worldwide.

55 Consumers' International, Shop Online 2001: An International Comparative Study of Electronic Commerce, September 2001 available at http://www.consumersinternational.org/CI_Should_I_buy.pdf

56 Bob Cohen, "New Poll Finds Americans Concerned About Security of Government Computers", Infosec Outlook, vol. 1 n.7 (September 2000) available at http://www.itaa.org

These surveys and reports confirm that building trust in the information society does not centre exclusively around security functionalities but derives from many other factors whose quantification is difficult. This variety of components undermines each of the three major qualities of any benchmark:

- representative
- useful
- agreed

Since a benchmark is an abstraction, it is bound to be an imperfect representation of reality. The challenge is to define a benchmark that is useful in representing a particular domain. More importantly, it has to be an instrument upon which different actors can agree. The multi-faceted and multi-dimensional nature of trust makes the use of trust as a benchmark very difficult.[57]

For example, it would be difficult to measure and compare the navigability or presentation style of e-commerce solutions or organisations. While it would be possible to create an *a priori* scale of values through which users might be asked to evaluate a site's navigation, presentation and usability,[58] any scale might reflect specific cultural, social, and gender biases.[59] At the same time, the navigability of a particular electronic commerce site may be improved not by the use of a particular web technology but as a result of improved availability of Internet access equipment, such as cable modems or ISDN lines.

Another example refers to the statistical assessment of the impact of regulation and legislation on overall trust towards the information society. As in the previous case, it is possible to perceive a situation where a region or a single country might devise very "trust-friendly" legislation, which is structured along the same lines as those of other countries. Still, in that country, Internet users might not have access to advanced communication technologies and services and hence will actually experience poor online services.

Although these are just two examples highlighting the complexity of establishing a single "trust indicator", the same problems arise when considering other "trust-enhancing" factors.

## *5.1 Summary*

This section has rejected the use of a single indicator measuring trust due to the multi-dimensional nature of trust. The nature of trust in the online environment prevents us from devising a single, measurable benchmark.

---

57 Some initial research has been completed on ways to formalise trust inside artificial agents. In this case, the goal is to develop software codes that might create agents whose actions can be trusted. See Stephen Paul Marsh, Formalising Trust as a Computational Concept, PhD Dissertation completed at the Department of Computer Science and Mathematics, University of Stirling, April 1994.

58 See Boyd De Groot and Florian Egger, "Designing For Trustworthiness: The Case of www.euclix.nl". Paper presented at the Computer Human Interface Workshop 2000: Designing Interactive Systems for 1-to-1 E-Commerce, The Hague, Netherlands, 1-6 April 2000

59 Sirkka L. Jarvenpaa and Noam Tractinsky, "Consumer Trust in an Internet Store: A Cross-Cultural Validation", Journal of Computer Mediated Communication, vol. 5 no.2 (December 1999) available at http://www.ascusc.org/jcmc/vol5/issue2/

# 6 Identification of Units of Analysis and their Role in the Context of Security

The previous section argued for the discarding of trust as a useful statistical indicator due to its multi-dimensional and multi-faced nature. Instead, it is proposed that we should concentrate on devising indicators measuring security. Before expanding on this, it is important to define the units of analysis that will be addressed by these security indicators.

The following may be considered as the primary units of analysis:

- Governments
- Industry
- Individuals

Each unit, however, does not have a single and well-defined role when it comes to security. As discussed in the remainder of this section, they are both providers and receivers of security functionalities. As argued below, this double role or function is essential and needs to be reflected in the drafting of surveys among the general population (GPS) and decision makers (DMS).

## *6.1 Governments*

*Governments* are users of IT and other electronic services as part of their efforts to improve their operations and the delivery of their services. At the same time, they are also providers of electronic goods and services. An interesting example is the case of a tax service providing licences for the use of proprietary software solutions to businesses so that they can file taxes electronically. Another example could be the provision of electronic identification cards, which allow citizens to access different public and private services.[60]

## *6.2 Industry*

*Industry* as a whole has always been a keen user of IT and other electronic services to try to contain costs and improve efficiency. In addition, there are sections of industry that focus on devising solutions to cater for the commercial and operational needs of public and private organisations. Meanwhile, there are organisations whose main function is to provide assistance in exploiting the functionalities and operational capabilities of hardware and software solutions by providing consultancy services. These may range from system integration and management to IT strategy development.

These categorisations are not static but dynamic. There are many cases of software developers who provide consultancy services to clients or user groups. Similarly, there are also many cases of companies that have a particular expertise in employing specific IT

[60] An interesting example is the case of the Finnish Electronic Identification and Supporting Technologies Programme. The goal is to provide Finnish citizens with an ID smart card, which includes digital signatures. Through this card, it is possible to access a large variety of social services, as well as private sector services such as bank accounts and entertainment events. For more information see Ms. Tuire Saaripuu, Population Register Centre, Finland, "Finnish Electronic Identification and Supporting Technologies Programme" Presentation at the OECD Workshop: Information Security in a Networked World, Tokyo, 12-13 September, 2001 available at http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-13-nodirectorate-no-20-18803-13,FF.html. An overview of similar initiatives is provided in Andreas Mitrakas, Laurent Blivet and Moise Moyal, "A Pre-Inventory of Smart Card Based PKI Projects within the EU" Report prepared as part of the E-Europe, Trailblazer 2-Identification and Authentication, November 2002.

solutions and decide to "sell" their expertise by launching professional services.[61] Finally, it is common for a particular company to begin to operate in a particular sector before deciding to abandon it to exploit the potentialities offered in another field. This dynamism is particularly evident in the information and communication industry where companies have moved from being hardware/software developers to providers of mobile and wireless telephony and data services. [62]

### 6.3 Individuals

*Individuals* are the third potential unit of analysis. They can be categorised in four different ways. Some individuals are *active users* by either buying or selling services and goods over the Internet. *Users* can also be *passive* as they merely access online services to collect information and data. This may be a "transitory" phase since it is possible that they gather data to carry out online transactions. *Users* may also be individual software and hardware providers, as in the case of the *open source* movement. Finally, *users* can also turned into *information providers* by devising their own websites or other forms of web-presence.

### 6.4 Summary

Although it is possible to argue that the above units of analysis as a whole appreciate security, each one has a specific individual perspective on this matter based on their particular operational objectives. This differentiation leads to qualitative and quantitative difficulties in structuring the data collection process through general public (GPS) and decision-making (DMS) surveys. For example, government officials involved in electronic government programmes will have different perspectives on security depending upon the criticality and nature of their services. Likewise, some industries will view security as a burden imposed, for instance, by regulatory mandates. At the same time, there are companies that have a commercial interest in promoting security since this will provide them with business opportunities.

Current indicators do not provide a clear specification of the particular unit of the analysis. For example, the CSI *Computer Crime and Security Survey* collects information directly from computer security specialists of US corporations, medical institutions and universities. The results, consequently, should provide a general overview of the status of information security and "cyber-crime" in the United States. Nevertheless, the results do not address information concerning each of the industry actors. More importantly, the results do not allow for comparisons between sectors.

## 7 Security Indicators

In order to address the difficulties highlighted above, a possible starting point is to concentrate on the following three indicators due to their direct relevance to security functionalities:

- Online Malicious Activities

[61] An interesting example is Italy's car manufacturer and conglomerate FIAT, which has spun off its human resource division as a separate company. This new entity is expected to provide consultancy services to companies outside the FIAT group.

[62] An interesting example is Italy's Olivetti. It began as a provider of office automation equipment before turning into a telecommunication service provider through the acquisition of a controlling stake in Telecom Italia. Presently, Italy's Pirelli, which is a leading manufacturer of telecommunications and data cables and tires, controls Telecom Italia. Each one of these changes has led to a re-focus of Telecom business strategy and interests with direct implications for their security needs and objectives.

- Prevention of Malicious Activities and Downtime
- Online Interactions Facilitators

## 7.1 On-line malicious activities

As indicated in SIBIS WP 2.1, there are a large variety of available indicators concerning online malicious activities provided by public and private organisations. Nevertheless, definitions and metrics are neither standardised nor incorporated into one single report.

A starting point would be to categorise data and to organise data collection according to the offences indicated in the forthcoming Convention on Cybercrime of the Council of Europe.[63] This document aims to harmonise substantive and procedural legislative measures in the area of cybercrime. The convention is expected to influence the development of national and European-wide legislation and perhaps also global legislation.[64] The convention refers to criminal activities and behaviours that may relate to the activities of many units of analysis.

However, the cybercrime convention does not address several important Internet-based criminal activities. In the case of copyright violations, data collection and analysis should be based on the offences indicated, for example, by the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations, the Agreement on Trade-related Aspects of Intellectual Property Rights and the World Intellectual Property Organisations (WIPO).[65]

Notwithstanding the terms of reference provided by these legal instruments, it is often the case that online malicious activities cannot always be defined as such. A possible solution would be to classify malicious activities as “attacks”. According to the *Incident Taxonomy and Description Working Group*, which is part of the TERENA Computer Security and Incident Response Teams Coordination (TCSIRT-C), an attack can be defined as:

> *an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. Attack can be active or passive, by insider or by outsider, or via attack mediator.*[66]

Whatever definitions are adopted, the main difficulty is to actually collect the necessary data.[67] As mentioned, public and private organisations are often reluctant to provide data about malicious activities, unless particular legal and contractual assurances about anonymity and non-disclosure are provided.[68] Information Sharing and Analysis Centres (ISACs), computer emergency response teams (CERTs) or computer security incident response teams

63 The final text is available at http://conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm

64 See Commission of the European Communities: Communication from the Commission to the Council and the European Parliament: Proposal for a Council Framework Decision on Combating Attacks against Computer Systems (Draft, 24 April 2001). For discussions about this draft, see the report of the expert meeting held in June available at http://www.europa.eu.int/information_society/topics/telecoms/internet/crime/consulatation_doc/index_en.htm

65 For more information see World Intellectual Property Organisation (WIPO), “Primer on Electronic Commerce and Intellectual Property” May 2002 available at http://ecommerce.wipo.int/primer/index.html

66 See TERENA-CSIRT, “Taxonomy of the Computer Security Incident Related Terminology-Draft” available at http://www.terena.nl/task-forces/tf-csirt/iodef/docs/i-taxonomy_terms.html

67 For an overview on how to report incidents see TERENA CSIRT, “Questionnaire About Tools, Procedures and Practices Used by CSIRTs to Collect Incident Data/Evidence, Investigate and Track Incidents” available at http://www.terena.nl/task-forces/tf-csirt/tf-csirt-chiht-q.rtf. For an overview of various incident report procedures, see http://www.terena.nl/task-forces/tf-csirt/iodef/docs/BCPreport1.rtf

68 The CERT-Coordination Centre provides interesting data. See CERT-Statistics at http://www.cert.org/stats/cert_stats.html

(CSIRTs) and other organisations have been trying to overcome these concerns but their effectiveness is often difficult to assess.[69]

A possible solution to the challenge of meta-data definition and data collection would be to establish an independent central organisation whose task would be to devise standardised data collection procedures and provide the necessary safeguards. It is important to emphasise that the mission statement of this independent organisation would only be to provide solid quantitative and qualitative statistical analysis to measure the overall phenomenon of online malicious activities. This would require data to be sanitised before being voluntarily transferred to this independent organisation.

## *7.2 Prevention of Malicious Activities and Downtime*

While the previous indicators aimed at describing and quantifying online malicious activities, these indicators aim to examine the other side of the equation. They aim to provide a qualitative and quantitative measure of the investments of public and private institutions and individuals in enhancing security functionalities (confidentiality, integrity, availability, authentication and non-repudiation) of their online activities.[70]

Unlike the previous indicators, it is possible to argue that there are already some standardised indicators available. Many public and private institutions (government organisations or market research companies) collect data about software and hardware security expenditures. A large part of this data comes from examining sales of specific solutions such as encryption software, firewalls, anti-virus software. Still, there is a general lack of detailed data about investments of how public and private institutions manage their information security.

A possible solution would be to draw on both the IT auditing/management consultancy community and regulatory/supervisory bodies. The former has quantifiable methods for monitoring and assessing how institutions handle their IT solutions and overall infrastructures. This involves the assessment of security processes, both technical and managerial. Regulatory and supervisory bodies, meanwhile, require detailed analysis of both IT operations and structures as part of their compliance requirements. An interesting example are the securities market regulators to whom listed companies are mandated to provide regular reports to keep investors abreast of the risks associated with their investments. Especially in the case of listed electronic commerce industries, these reports provide detailed information about information security investments, IT budgets and sales figures.[71] More importantly, this data is validated by the fact that it is an offence for companies to provide false information.

There is still the need for specific standards for quantitative and qualitative data collection in this area. There are various options. First, it is possible to collect sales data about specific information security solutions and services. Second, it is possible to collect data about the percentage of an organisation's IT budget that is devoted to security. However, this data is not always readily available since IT security budgets are often spread across different sections of the overall IT budget of organisations.

A third option is to coordinate data collection processes with organisations involved in measuring the "dependability" of information and network systems providing transaction capabilities. These methods can be extremely useful especially in relation to the assessment of "downtime" or "service delivery failures". The Transaction Processing Performance Council (TPPC), a US-based non-profit organisation established by leading software and hardware producers, is a good example in this context.[72] The TPPC has devised two main benchmarks

[69] For an interesting overview, see Dependability Development Support Initiative (DDSI) and Joint Research Centre, "European Warning and Information System: Issues and Background Paper for Workshop, 25-26 October 2001" available at http://ewis.jrc.it

[70] Security measures both against malicious activities and unplanned downtime or service delivery breakdowns.

[71] See for example the quarterly report of Amazon.com, the leading Internet bookseller, available at http://www.iredge.com/IREdge/IREdge.asp?c=002239&f=2016

[72] For more information see http://www.tcp.org

to measure performance and price/performance of information systems and databases employed for online transaction functionalities.[73] The first is *TPC-C*. It simulates a complete transaction process system similar to those operating in a real environment by looking at, *inter alia*:

- Execution of multiple transactions
- Transaction integrity
- Database accesses and updates

The second benchmark, TCP-W, emulates the activities of an Internet commerce environment by assessing, *inter alia*:

- Multiple sessions
- Dynamic page generations
- Simultaneous execution of multiple transactions
- Database accesses and updates

TCP-W's most interesting functionalities are to simulate three different profiles: online shopping, browsing and web-based ordering. Each one presents different simulations of price and transaction volumes and, consequently, generates different sets of data.

Another possible indicator would involve the collection of data about service delivery levels provided by Internet or Application Service Providers (ASPs). These organisations may offer their clients services based on "Service Level Agreements". These are written arrangements spelling out the minimal acceptable service to be provided by an information service provider to a user. They may involve stringent requirements in terms of security and output requirements, as well as service level. [74]

These last two options, however, share a common methodological limitation. As with the case of online malicious activities, organisations and individuals are reluctant or not allowed to provide data about the dependability of their information and network systems, as well as their compliance to the terms of their service level agreements. This limitation may be overcome by establishing an independent organisation, whose task is to collect these data on a voluntary basis and in an anonymous manner.

## *7.3 Seals and Web-based Quality Certificates*

Seals are recognised standards certified by an auditing process involving checks on security and privacy provisions. During the last three years, there has been a proliferation of these initiatives, both in the United States and in Europe, launched by private and public sector bodies. A sample list includes:

- Better Business Bureau Code (US)
- BetterWeb (USA)
- Certisek (Italy)
- Clicksure (UK)
- ECOM (Electronic Commerce Promotion Council of Japan) Web Mark
- E-Commerce Quality Mark (Italy)
- E-Maerket (Denmark)

[73] See J.Arlat, K. Kanoun, H. Madeira, J.V. Busquets, T. Jarbouni, A. Johansson and R. Lindstrom, State of the Art, Report CF1-State of the Art-Dependability Benchmarking, EU-IST 2000-25425, pp. 42-45

[74] For an example of a service level agreement, see UUNET-World Com, Service Level Agreement for Virtual Private Network, at http://www.uu.net/terms/sla/emea/vpn.xml

- FEDMA (Federation of European Direct Marketing) Mark
- Q-Web (Italy)
- TrustE (USA)
- Web-Trade Code of Conduct (US)
- Webtrader (Italy)
- Webtrust (Italy)
- Which? Webtrader (UK)

Unlike the two previous indicators, these indicators do not present any difficulty concerning quantification. In the United States, the General Accounting Office (GAO) has conducted comprehensive surveys concerning the ways in which federal offices communicate their privacy and security policies and processes.[75] Meanwhile, ASSINTEL, Italy's leading organisation representing software and hardware developers, has completed an extensive survey measuring organisational attitudes towards web-quality certificates.

# 8 A Single or Three Separate Security Indicators?

The previous chapter has provided an overview of three possible indicators for benchmarking security. This section examines the possibility of combining these indicators into a single one. The argument is that this is not possible, unless all three are converted into a common denominator. As in the case of trust, this conversion process may lead to a benchmark that is not representative, useful or agreed upon by all interested parties.

Online malicious activities, prevention of malicious activities and downtime, and seals/web-based quality certificates refer to three different phenomena. This differentiation may be overcome through their conversion into financial measures. This would require financially quantifying the impact of online malicious activities or attacks. Some of the surveys listed in WP 2.1 have attempted to do so. However, as previously indicated, these surveys fail to define their units of analysis. This is pivotal since the financial quantification of these malicious activities depends on the overall business and IT objectives of each organisation. [76]

The Information Security Forum, an international industry group, has provided some guidelines in this regard. Its Information Security Survey 1999 concluded that online malicious activities might degrade organisations' performance, which might become visible to their customers. In this case, this degradation can have an "impact on overall profit" and "impact on business". The former refers the attack's impact on the company's profitability, whilst the latter measures the overall effect on the balance sheet.[77] Although these calculations can be carried out at the micro level, the situation becomes more complex at the macro level. It would require an approximation among public and private organisations, which use IT and other information and network technologies in different ways. The end result would be a benchmark that is not representative of the security of the Information Society. Similar concerns apply also to the other two proposed statistical indicators. As previously mentioned, it is possible to collect hard data about IT security investments and other activities. Nonetheless, there are still major difficulties in quantifying the business and operational

[75] For the GAO,see Internet Privacy: Comparison of Federal Agencies Privacy Policies, AIMD-00-296R, September 2000. For ASSINTEL, see:, "Sicurezza delle Transazione, Certificazione dei Siti Web and Firma Elettronica-2001", at http://www.assintel.it/Indagine.nsf/1bc98e482f20deb7c125678a00434795/2da960e5d113f26ec1256af6004e3328?OpenDocument.

[76] For more information see Broadbent, M. and Lofgren H., "Information Delivery: Identifying Priorities, Performance and Value", Information Processing and Management, vol. 29 n. 6, 1993, pp. 683 – 701, Taylor, A, and Farrell, F., Information Management for Business, (London: ASLIB Press, 1994). The authors would like to thank Neil Robinson, Associate Analyst, Rand Europe Cambridge for suggesting this aspect.

[77] Cited in Information Assurance Advisory Council (IAAC), "The Cost of Cybercrime", Briefing Paper 17, June 2001.

impact of these expenses. Similar arguments relate to seals and web-based quality certificates, whose commercial and business viability has not yet been reliably assessed.

The separation amongst these three security indicators has a positive impact on their use as benchmarks for tailoring European and national public policies aimed at fostering the overall security of the information society. The solution is for them to be examined individually but in a coordinated fashion, as demonstrated in the following example.

The benchmark for online malicious activities represents a particular overview of the state of affairs in this area at a particular point in time. Variations of this benchmark may lead to an assessment or re-consideration of those policies aimed at countering cybercrime, network intrusions, online paedophilia and/or digital copyright protection. Policy makers may react to these figures by either preserving the status quo or enacting new policies and regulations. The efficacy of new policies may be tested by the benchmark's variations. Online malicious activities, however, are just one side of security. Their negative implications may be prevented through appropriate security technical and managerial measures, which are quantified by the other two indicators examined in this report. Therefore it is possible to conceive of a situation in which policy makers may decide to enact policies to foster information security amongst individuals and organisations. It is possible that these new policy measures may lead to unnecessary new burdens on organisations without any visible impact on the number of online malicious activities. This state of affairs, which will be registered by the relevant benchmarks, may lead to a readjustment of policies.

These are just two of several combinations and possible policy analysis based on combinations amongst the three security indicators. Still, it is important to emphasise that, by keeping the three indicators separate but related, the benchmarking process of security will be facilitated.

# 9 Suggestions for compound indicators

The indicators emerging from the survey, at both GPS and DMS levels can be instructive to build compound indicators and helpful when it comes to benchmarking states (or demographic classes etc.) with regard to their performance or behaviour in the information society. By weighting single indicators according to their relevance for a certain issue, it is possible to construct such an index. These indices can be useful in informing policy, because they can assist in identifying strengths and weaknesses of the information society and in performing a SWOT analysis.

Indices may be built by weighting the results obtained in the DMS and the GPS on the different categories within the security indicators (e.g. concerns, awareness, information security strategy etc.), describing, among others, risk, security, secure behaviour etc. undergone by different demographic categories or states.

Just as examples, a "risk index", could assess the risk of suffering breaches in different countries, a "security index" could, on the contrary show how secure different countries are. Similarly, based on different GPS indicators, a "behaviour index" might describe how different categories perceive the trustworthiness of the information society.

# 10 Conclusion

This report opened by arguing for the dismissal of a single statistical indicator combining trust, confidence and security. The reasons were that the multidimensional and multi-faceted structure of trust in an online environment do not allow for the definition of a single benchmark indicator that is representative, useful and agreed upon amongst all the interested parties. Subsequently, the paper examined three potential statistical indicators of security:

- Online malicious activities

- Prevention of online malicious activities and downtime
- Seals and web-based quality certificates.

This report argued for the need to keep these three indicators separate. This is due to the fact that they represent different domains. However, this separation does not impinge upon their overall usefulness. As long as they are interpreted and examined in parallel, the three proposed statistical indicators can provide a useful tool for policy makers to devise appropriate policies aimed at fostering the security of the information society.

# 11 New indicators

## 11.1 Overview of new indicators

| No. | Name of indicator | Based on | Method |
|---|---|---|---|
| 1 | Security Breaches Occurred in the Organisation | GVU<br>Eurobarometer 2001<br>Information Security Industry Survey | SIBIS DMS |
| 2 | Types of Breaches Suffered | GVU<br>Eurobarometer 2001<br>Information Security Industry Survey | SIBIS DMS |
| 3 | Supposed Origin of Breaches | GVU<br>Eurobarometer 2001<br>Information Security Industry Survey | SIBIS DMS |
| 4 | Source of Information on Occurred Breaches | GVU<br>Eurobarometer 2001<br>Information Security Industry Survey | SIBIS DMS |
| 5 | Importance attributed to Information Security | GVU<br>Eurobarometer 2001<br>Information Security Industry Survey | SIBIS DMS |
| 6 | Information Security Priorities | GVU<br>Eurobarometer 2001<br>Information Security Industry Survey | SIBIS DMS |
| 7 | Presence of Information Security Policy | Information Security Industry Survey | SIBIS DMS |
| 8 | Sort of Information Security Policy | Information Security Industry Survey | SIBIS DMS |
| 9 | Alignment of Security Policies to Organisations' Objectives | - | SIBIS DMS |
| 10 | Barriers to Information Security | Securitystats.com | SIBIS DMS |
| 11 | Tools of Information Security | Information Security Industry Survey | SIBIS DMS |
| 12 | Comprehension of Private Sectors' Security Requirements by the Public Sector | - | SIBIS DMS |
| 13 | Co-operation of private sector in fostering information security | - | SIBIS DMS |
| 14 | Concern Regarding On-line Security | GVU<br>Gallup Organisation | SIBIS GPS |
| 15 | Concern Regarding On-line Privacy and Confidentiality | GVU<br>Gallup Organisation | SIBIS GPS |
| 16 | Effect of Security Concerns on On-line Shopping Behaviour | Privacy@net, study of Consumers International | SIBIS GPS |

| No. | Name of indicator | Based on | Method |
|---|---|---|---|
| 17 | Propensity to Report Incidents of On-line Violation | GVU | SIBIS GPS |
| 18 | Propensity to Report Incidents of On-line Violations, Under Assurance of Anonymity | GVU | SIBIS GPS |
| 19 | Awareness of security features of websites | Eurobarometer 2001 | SIBIS GPS |
| 20 | Effects of perceived security features on consumers' propensity to shop on-line | Eurobarometer 2001 | SIBIS GPS |
| 21 | Quality Assurance and Commitment of On-line Merchants to Security | - | SIBIS GPS |
| 22 | Companies' Information About On-line Security | - | SIBIS GPS |
| 23 | Need for Information on Security and Vulnerabilities | - | SIBIS GPS |
| 24 | Organisations Which Can Offer the Information needed | - | SIBIS GPS |

## *11.2 Description of new indicators*

| Name of indicator | Security Breaches Occurred in the Organisation |
|---|---|
| Definition | Percentage of businesses which have suffered security breaches in the last year |
| Notes | - |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Eurobarometer 2001<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>Have any security breaches occurred in your organisation in the last 12 months?<br>• Yes<br>• No<br>• Do not know |
| eEurope relevance | 1c-1 |

| Name of indicator | Types of Breaches Suffered |
|---|---|
| Definition | Percentage of breaches suffered, by different categories |
| Notes | - |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Eurobarometer 2001<br>Information Security Industry Survey |
| SIBIS survey: Q and | Target Group: DMS |

| | |
|---|---|
| group to be asked | If yes, which of the following types of security breaches have occurs in your establishment in the last 12 months? Did you experience cases of…<br>• Identity Theft<br>• On-line Fraud<br>• Manipulation of Software Applications<br>• Computer Virus Infections<br>• Unauthorised Entry to Internal Networks |
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Supposed Origin of Breaches** |
|---|---|
| Definition | Main origin of security breaches according to the statement of IT decision makers in businesses |
| Notes | - |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Eurobarometer 2001<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>Where do you believe these breaches mainly came From? Do you think the largest threat to on-line security came from…<br>• Customers<br>• Suppliers/Competitors<br>• Former Employees<br>• Computer Hackers<br>• Internal Users<br>• Others, not mentioned yet<br>• DK |
| eEurope relevance | 1c-1; 1c-3 |

| **Name of indicator** | **Source of Information on Occurred Breaches** |
|---|---|
| Title | - |
| Definition | Main source of Information on Occurred Breaches according to IT decision makers in businesses |
| Notes | This question assesses how organisations become aware about their breaches. This information is important in reference to early warning and information sharing |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Eurobarometer 2001<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>How have you learned about these breaches, in most cases? Were you…<br>• Alerted by a customer/supplier |

| | |
|---|---|
| | • Alerted by employees<br>• Notified by your own information security system<br>• Made aware by damage or loss of dataAlerted by the providers of outsourced security services |
| eEurope relevance | 1c-3 |

| **Name of indicator** | **Importance attributed to Information Security** |
|---|---|
| Definition | - |
| Notes | This question aims to assess what importance organisations attribute to information security, according to the perception of IT decision makers |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Eurobarometer 2001<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>What priority does information security have in your organisation?<br>• High<br>• Medium<br>• Low<br>• Insignificant |
| eEurope relevance | 1c-1; 1c-3 |

| **Name of indicator** | **Information Security Priorities** |
|---|---|
| Title | - |
| Notes | Multiple answers allowed; optional: Ask for ranking |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Eurobarometer 2001<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>Which are your information security priorities? How much priority is given to<br>•<br>•<br>• Blocking of Unauthorised Access<br>•<br>• Expanding Budget for Security Measures<br>• Defining the Security Architecture<br>• Outsourcing security management |
| eEurope relevance | 1c-1; 1c-3 |

| **Name of indicator** | **Presence of Information Security Policy** |
|---|---|
| Definition | |
| Notes | |
| Sources | Based on<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>Does your establishment or your organisation have an information security policy?<br>• Yes<br>• No<br>• DK |
| eEurope relevance | |

| **Name of indicator** | **Sort of Information Security Policy** |
|---|---|
| Definition | This question aims to assess the "quality" of information security policies. |
| Notes | The question assumes that the surveyed organisation has some kind of information security policy in place, which should be investigated beforehand in a separate question. |
| Sources | Based on<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>How would you describe your information security policy?<br>• Formal<br>• Informal<br>• DK |
| eEurope relevance | |

| **Name of indicator** | **Alignment of Security Policies to Organisations' Objectives** |
|---|---|
| Definition | Percentage of organisations whose decision makers consider the level of alignment of security policies to the organisations' operational and business objectives satisfactory (or not) |
| Notes | |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>How well are the structures and the funding of your security policies aligned with the operational and business objectives?<br>• Completely aligned<br>• Somewhat aligned<br>• Closely aligned<br>• Poorly aligned<br>• Not aligned |
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Barriers to Information Security** |
|---|---|
| Definition | Factors undermining the implementation of information security policies inside organisations, according to the statements of IT decision makers |
| Notes | - |
| Sources | Based on Securitystats.com (Computer security news) |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>How important are the following factors as barriers to effective information security inside an organisation?<br>• High costs for security measures<br>• Lack of staff training<br>• Lack of staff time<br>• Complexity of the Technology<br>• Lack of employee co-operation |
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Tools of Information Security** |
|---|---|
| Definition | Information security technologies in use by organisations, in % by category |
| Notes | - |
| Sources | Based on<br>Information Security Industry Survey |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>Which of The following Tools Do You Use for Information Security in your establishment? Do you make use of<br>• Controls of access to the computer system<br>• Cryptography/ data encryption<br>• Vulnerability Assessment Tools<br>• Firewalls<br>• Security Training and Awareness Rising Activities<br>• Intrusion Detection Systems<br>• End-user Security Training Classes |
| eEurope relevance | - |

| **Name of indicator** | **Comprehension of Private Sectors' Security Requirements by the Public Sector** |
|---|---|
| Definition | % of private organisations that consider satisfactory (or not) the level of comprehension of their security needs by the public sector |
| Notes | Specific question for DM from the private sector |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>Do you believe that public institutions have a clear understanding of the information security requirements of the private sectors?<br>• Not at all<br>• Partially<br>• Yes |
| eEurope relevance | 1c-3 |

| **Name of indicator** | **Co-operation of private sector in fostering information security** |
|---|---|
| Definition | - |
| Notes | Specific question for DM from the public sector |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: DMS<br>How would you rate the co-operation of private sector in fostering information security for Europe's information society?<br>Very effective<br>Effective<br>Insufficient<br>Not available |
| eEurope relevance | 1c-1; 1c-3 |

| **Name of indicator** | **Concern Regarding On-line Security** |
|---|---|
| Definition | Percentage of population aged 25-64 expressing concerns about on-line security, confidentiality and privacy |
| Notes | Respondents are supposed to be able to surf on the Internet |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Study conducted by the Gallup Organisation (Internet Privacy Survey, 2000 ) |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet use)<br>How concerned are you about data security on the internet?<br>• Very concerned<br>• Somewhat concerned<br>• Not concerned<br>• DK |
| eEurope relevance | 1c-x |

| **Name of indicator** | **Concern Regarding On-line Privacy and Confidentiality** |
|---|---|
| Definition | Percentage of population aged 25-64 expressing concerns about on-line confidentiality and privacy |
| Notes | Respondents are supposed to be able to surf on the Internet |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology<br>Study conducted by the Gallup Organisation (Internet Privacy Survey, 2000 ) |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet use)<br>How concerned are you about privacy and confidentiality on the Internet, i.e. personal information about you being misused by third parties?<br>• Very concerned<br>• Somewhat concerned<br>• Not concerned<br>• DK |
| eEurope relevance | 1c-x |

| **Name of indicator** | **Effect of Security Concerns on On-line Shopping Behaviour** |
|---|---|
| Definition | Percentage of population aged 25-64 who limit their on-line transactions as a consequence of security concerns |
| Notes | - |
| Sources | Based on Privacy@net, study of Consumers International |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet users)<br>Are security or privacy concerns stopping you from using the Internet to buy goods or services on-line: often, sometimes or never?<br>• Often<br>• Sometimes<br>• Never<br>• DK |
| eEurope relevance | 1c-x |

| **Name of indicator** | **Propensity to Report Incidents of On-line Violation** |
|---|---|
| Definition | Percentage of population aged 25-64 who would report violations of their on-line security, privacy and confidentiality without specific assurance of anonymity. |
| Notes | - |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet users)<br>Would you report violations of your on-line security, privacy and confidentiality to a third independent party, for example a public agency created for this task?<br>• Yes, very likely |

| | |
|---|---|
| | • Maybe<br>• No<br>• DK |
| eEurope relevance | 1c-3 |

| **Name of indicator** | **Propensity to Report Incidents of On-line Violations, Under Assurance of Anonymity** |
|---|---|
| Definition | Percentage of population aged 25-64 who would report violations of their on-line security, privacy and confidentiality with specific assurance of anonymity. |
| Notes | - |
| Sources | Based on<br>Surveys conducted by GVU-Georgia Institute of Technology |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet users)<br>Would it be easier for you to report violations of your on-line security, privacy and confidentiality anonymously?<br>• Yes<br>• Not<br>• DK |
| eEurope relevance | 1c-3 |

| **Name of indicator** | **Awareness of security features of websites** |
|---|---|
| Definition | |
| Notes | |
| Sources | Based on Eurobarometer 2001 |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet users)<br>How often are you aware of security features of websites when you use the Internet to buy on-line: often, sometimes or never?<br>• Often<br>• Sometimes<br>• Never<br>• DK |
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Effects of perceived security features on consumers' propensity to shop on-line** |
|---|---|
| Definition | Relation between security features and consumers' propensity to shop on-line |
| Notes | - |
| Sources | Based on Eurobarometer 2001 |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet users)<br>How often do you take security features of websites into account when deciding about whether to buy on-line: often, sometimes or never?<br>• Often<br>• Sometimes<br>• Never<br>• DK |
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Quality Assurance and Commitment of On-line Merchants to Security** |
|---|---|
| Definition | Percentage of population aged 25-64 valuing a link between seals of trust and/or certificates of quality and the commitment of an on-line store or merchant to on-line security, privacy and confidentiality |
| Notes | Respondents are supposed to be able to surf on the Internet |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: GPS (Internet users)<br>Do you think seals of trust and/or certificates of quality would assist in assessing the commitment of an on-line store or merchant to on-line security, privacy and confidentiality?<br>• Yes<br>• Not<br>• Do not care |
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Companies' Information About On-line Security** |
|---|---|
| Definition | Percentage of population aged 25-64 assessing companies' information about their on-line security and commitment to on-line security and privacy as sufficient (or not) |
| Notes | - |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: GPS<br>In your experience, do companies always give sufficient information about their on-line security and commitment to on-line security and privacy?<br>• Yes<br>• Not<br>• DK |

| | |
|---|---|
| eEurope relevance | 1c-1 |

| **Name of indicator** | **Need for Information on Security and Vulnerabilities** |
|---|---|
| Definition | Percentage of population aged 25-64 expressing the need (or not) of further information concerning security and vulnerabilities |
| Notes | The next question deals with the possible bodies offering this information |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: GPS<br>Would you like to receive information about security vulnerabilities?<br>• Yes<br>• Not<br>• DK |
| eEurope relevance | 1c-x |

| **Name of indicator** | **Organisations Which Can Offer the Information needed** |
|---|---|
| Definition | Percentage of population aged 25-64 who would prefer to receive information on security and vulnerabilities from public (or private) organisations |
| Notes | - |
| Sources | - |
| SIBIS survey: Q and group to be asked | Target Group: GPS<br>If yes: would you prefer to receive from a public (government institutions) or private organisations (software and hardware producers or Internet Service Providers?<br>• Public organisation<br>• Private organisation |
| eEurope relevance | 1c-x |

# 12 Annexes

## 12.1 Review of traditional indicators[78]

*Overview Table*

| No. | Name of indicator | Sub-domain | eEurope code | Main Source |
|---|---|---|---|---|
| A1 | Internet users encountering problems | Trust and Security | 1c-x | Eurobarometre Feb. 2001 |
| A2 | Security features adopted by computer owners | Trust and Security | 1c-x | Eurobarometre Feb. 2001 |
| A3 | Persons who have ordered a good or a service over the Internet | Trust and Security | 1c-1 | Eurobarometre Feb. 2001 |
| A4 | Number of security incidents in the Netherlands | Trust and Security | 1c-x | Surfnet-NL |
| A5 | Sixth Computer Crime and Security Survey | Trust and Security | 1c-1 | CSI |
| A6 | Fraud categories | Trust and Security | 1c-1 | IFCC |
| A7 | Financial losses | Trust and Security | 1c-1 | IFCC |
| A8 | Type and gender of Internet fraud perpetrators | Trust and Security | 1c-3 | IFCC |
| A9 | Type, gender and age of complainants | Trust and Security | 1c-3 | IFCC |
| A11 | Customer Preference to On-line or Off-line Shopping | Trust and Security | 1c-1 | CyberAtlas/cPulse |
| A12 | Internet Use 1998 vs. 2000 | Trust and Security | 1c-1 | CyberAtlas |
| A13 | Computer Security Spending Statistics –July 1999 | Trust and Security | 1c-1 | SecurityStats.com |
| A14 | Primary Use of the Web | Trust and Security | 1c-x | GVU-Georgia Institute of Technology |
| A16 | Number of Secure Web Servers | Trust and Security | 1c-x | OECD Netcraft Survey- July 2000 |
| A17a | Portion of job responsibilities devoted to infosecurity | Trust and Security | 1c-x | Information Security Industry Survey |
| A17b | Security budget trends | Trust and Security | 1c-x | Information Security Industry Survey |
| A17c | Concerns and programs | Trust and Security | 1c-x | Information Security Industry Survey |
| A17d | Security breaches | Trust and Security | 1c-x | Information Security Industry Survey |
| A17e | E-commerce activity | Trust and Security | 1c-x | Information Security Industry Survey |
| A17f | Security controls | Trust and | 1c-x | Information Security |

[78] These indicators are termed “traditional” for any one or more of three reasons. First they derive from a source that carries out such surveys on a periodical basis. Traditional indicators also come from an organisation that itself is well established and consequently have a reputation for reliability and authenticity. Finally, traditional sources are characterised by their subject matter insofar as fraud, for example, might be understood as a traditional crime wherever it is taking place.

| No. | Name of indicator | Sub-domain | eEurope code | Main Source |
|---|---|---|---|---|
| | | Security | | Industry Survey |
| A18 | Computer crime - arrests and convictions | Trust and Security | 1c-x | Criminal division of US division of justice |
| A19 | Fraud and Security update | Trust and Security | 1c-1 | Professional Communications Security Management Journal |
| A20 | Cross-border eCommerce complaints | Trust and Security | 1c-1<br>1c-3 | econsumer.gov |

*Indicator descriptions in detail*

| **Name of indicator** | **A1 Internet users encountering problems** |
|---|---|
| Definition | Percentage of persons who have encountered one of the following problems while using the Internet:<br>• unsolicited E-mails<br>• viruses<br>• harassment or offensive offers<br>• credit card number abuse |
| Notes | This indicator has a broad applicability to the issue of Security and Trust since it measures various forms of problems occurring |
| Sources | Eurobarometer February 2001 |
| Countries covered | All EU countries |
| Time series available | - |
| eEurope relevance | • 1c-1<br>• 1c-3<br>• 1c-x |
| Future value | Supposedly this indicator will have little/no significance in 3/5/10 years from now and will need frequent updating, considering the speed of the so called “Internet years[79]” |
| Links to other indicators | - |

[79] An “Internet year” is a term commonly used to mean three calendar months, National Plan for Information Systems Protection, USA, January 2000

| **Name of indicator** | **A2 Security features adopted by computer owners** |
|---|---|
| Definition | Kinds of security features adopted by those who own a computer or a laptop. |
| Notes | This indicator was made by listing a number of possible security features to the interviewees giving a "yes or no" answering option, not by asking them what security features they actually possessed and creating a percentage from there. The options included:<br>• Anti-virus software<br>• Smart card reader or other<br>• An encryption software<br>• A firewall software<br>• Electronic signature software<br>• Other<br>• None of these |
| Sources | Eurobarometer February 2001 |
| Countries covered | All EU countries |
| Time series available | - |
| eEurope relevance | 1c-x |
| Future value | Supposedly this indicator will have little/no significance in 3/5/10 years from now and will need frequent updating, considering the speed of the so called "Internet years80". |
| Links to other indicators | - |

| **Name of indicator** | **A3 Persons ordering a good or a service over the Internet** |
|---|---|
| Definition | Percentage of persons who have ordered a good or a service on the Internet |
| Notes | - |
| Sources | Eurobarometer February 2001 |
| Countries covered | All EU countries |
| Time series available | - |
| eEurope relevance | 1c-1 |
| Future value | - |
| Links to other indicators | - |

[80] See note 5.

| **Name of indicator** | **A4 Number of security incidents in the Netherlands** |
|---|---|
| Definition | Absolute number of security incidents in Netherlands during year 2000, and change to previous year |
| Notes | The indicator refers the total number of incidents actually reported. This significantly increased due also to increased activity on the Internet and greater awareness. Also, the total number is broken down into different sorts of incidents, namely:<br>• Other unauthorised use<br>• Denial of service<br>• Probes |
| Sources | Surfnet-NL, Annual report 2000 |
| Countries covered | The Netherlands |
| Time series available | Annual |
| eEurope relevance | 1c-x |
| Future value | Supposedly this indicator will have little/no significance in 3/5/10 years from now and will need frequent updating, considering the speed of the so called “Internet years81 |
| Links to other indicators | |

| **Name of indicator** | **A5 Financial losses due to computer breaches** |
|---|---|
| Definition | Percentage of computer security practioners who have acknowledged financial losses due to computer breaches, and amount of such losses. |
| Notes | Based on responses from 538 computer security practitioners in US corporations, government agencies, financial institutions, medical institutions and universities. |
| Sources | Sixth Computer Crime and Security Survey; Computer Security Institute (San Francisco-USA). The annual survey offers a general overview of cyber problems encountered.82 |
| Countries covered | USA |
| Time series available | Annual |
| eEurope relevance | 1c-1 |
| Future value | - |
| Links to other indicators | - |

81 See note 5

82 The full “Computer Crime and Security Survey” can be requested in paper copy, free of charge

| **Name of indicator** | **A6 Incidents of fraud over the Internet** |
|---|---|
| Definition | Different categories of fraud over the Internet as percentage of all incidents of fraud over the Internet (May-November 2000)<br>• Auction fraud<br>• Non deliverable<br>• Credit- debit card fraud<br>• Other types of confidence fraud<br>• Investment fraud<br>• other |
| Notes | Based on complaints received by IFCC, directly between IFCC and US internet users |
| Sources | Internet Fraud Compliant Centre (USA) |
| Countries covered | USA |
| Time series available | Six-monthly |
| eEurope relevance | • 1c-1<br>• 1c-3 |
| Future value | Supposedly this indicator will have little significance in 3/5/10 years' time. |
| Links to other indicators | A5<br>A3 |

| **Name of indicator** | **A7 Financial losses resulting from fraud over the Internet** |
|---|---|
| Definition | Percentage of referrals by $ loss.<br>• below 100 $<br>• 100 $ to 499 $<br>• 500 $ to 999 $<br>• 1,000 $ to 2499 $<br>• 2,500 $ to 4,499 $<br>• 5,000 $ to 10,000 $<br>• over 10,000 $ |
| Notes | Based on complaints received by IFCC |
| Sources | Internet Fraud Compliant Centre (USA) |
| Countries covered | USA |
| Time series available | Six-monthly |
| eEurope relevance | 1c-1 |
| Future value | Supposedly this indicator will have little significance in 3/5/10 years' time. |
| Links to other indicators | A5 |

| **Name of indicator** | **A8 Type and gender of Internet fraud perpetrators** |
|---|---|
| Definition | Internet fraud perpetrators broken down by type and gender<br>• Individual only<br>• Individual and business<br>• Business only |
| Notes | Based on complaints received by IFCC |
| Sources | Internet Fraud Compliant Centre (USA) |
| Countries covered | USA |
| Time series available | Six-monthly |
| eEurope relevance | • 1c-1<br>• 1c-3 |
| Future value | Supposedly this indicator will have less significance in 3/5/10 years' time. |
| Links to other indicators | |

| **Name of indicator** | **A9 Type, gender and age of complainants** |
|---|---|
| Definition | Categories of complainants who suffered Internet fraud<br>• Business vs individual<br>• Female vs male<br>• below 20, 20-29, 30-39, 40-49, 50-59, 60-69,70-79, 80 and older |
| Notes | Based on complaints received by IFCC |
| Sources | Internet Fraud Compliant Centre (USA) |
| Countries covered | USA |
| Time series available | Six-monthly |
| eEurope relevance | • 1c-1<br>• 1c-3 |
| Future value | Supposedly this indicator will have less significance in 3/5/10 years' time. |
| Links to other indicators | A8 |

| **Name of indicator** | **A11 Customer Preference to On-line or Off-line Shopping** |
|---|---|
| Definition | Indicates (in %) what sort of shopping the consumer would chose (for each of a list of categories), if an item is easy to buy both off-line and on-line.<br>• Apparel<br>• electronics<br>• Travel<br>• Books/video<br>• Groceries<br>• Investing<br>"Easy" means that you can choose on an equal basis to buy the good on-line or off-line (with the same amount of effort) |
| Notes | Internet survey of 2000/11/27 |
| Sources | CyberAtlas/cPulse (http://cyberatlas.Internet.com/) |
| Countries covered | USA |
| Time series available | No |
| eEurope relevance | 1c-1 |
| Future value | Supposedly this indicator will have less significance in 3/5/10 years' time. |
| Links to other indicators | A6; A7 |

| **Name of indicator** | **A12 Internet Users' preferences for different sorts of E-commerce 1998 vs. 2000** |
|---|---|
| Definition | Indicates what sort of e-commerce Internet users prefer, comparing year 2000 to 1998<br>• Shopping on-line 1998 vs 2000<br>• Banking on-line 1998 vs 2000<br>• Trading stocks 1998 vs 2000<br>• Booking travel reservations or tickets 1998 vs 2000 |
| Notes | Internet survey of 2000/10/25 |
| Sources | CyberAtlas (http://cyberatlas.Internet.com/) |
| Countries covered | USA |
| Time series available | No |
| eEurope relevance | 1c-1 |
| Future value | Supposedly this indicator will have less significance in 3/5/10 years' time |
| Links to other indicators | A6; A7; A10 |

| **Name of indicator** | **A13 Computer Security Spending Statistics –July 1999** |
|---|---|
| Definition | Measures the obstacles to achieving adequate information-security organisations |
| Notes | The 1999 Industry Survey was completed by 745 Information Security readers, a pool of respondents that includes administrators, managers and executives in IT, security, networking and data management |
| Sources | Computer Security Spending Statistics – July 1999; SecurityStats.com (http://www.securitystats.com) |
| Countries covered | USA |
| Time series available | No |
| eEurope relevance | 1c-1 |
| Future value | Supposedly this indicator will have less significance in 3/5/10 years' time |
| Links to other indicators | A2; A5; A7 |

| **Name of indicator** | **A14 Primary Uses of the Web** |
|---|---|
| Definition | Measures the different uses of the web by Internet users, broken down by Gender, Age, Experience, Skill level.<br>Uses are:<br>• Education<br>• Shopping<br>• Entertainment<br>• Work<br>• Communication<br>• Personal information<br>• Time wasting<br>• OtherLocation |
| Notes | - |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998<br>GPS.<br>Since there is no centralised registry of all users of the Internet and users are spread out all over the world, it becomes quiet difficult to select users of the entire population at random. To simplify the problem most surveys of the Internet focus on a particular region of users, which is typically the United States, though surveys of European, Asian, and Oceanic users have also been conducted. |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **A16 Secure Web Servers** |
|---|---|
| Definition | Number of secure Web servers per 100,000 persons |
| Notes | - |
| Sources | OECD netcraft Survey, July 2000, in Network and Information Security: Proposal for a European Policy Approach |
| Countries covered | OECD countries |
| Time series available | Not specified, but supposedly three/six monthly |
| eEurope relevance | 1c-x |
| Future value | Supposedly this indicator will have less significance in 3/5/10 years' time |
| Links to other indicators | - |

| **Name of indicator** | **A17a Portion of job responsibilities devoted to infosecurity** |
|---|---|
| Definition | Portion of job responsibilities devoted to infosecurity<br>• Part<br>• all<br>• None |
| Notes | - |
| Sources | Information Security Industry Survey<br>http://www.infosecuritymag.com/ |
| Countries covered | USA |
| Time series available | Periodically |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| **Name of indicator** | **A17b Security budget trends** |
|---|---|
| Definition | Security budgets (broken down by industry (Consulting, banking/finance, high-tech, military, other) and by company size. |
| Notes | - |
| Sources | Information Security Industry Survey<br>http://www.infosecuritymag.com/ |
| Countries covered | USA |
| Time series available | Periodically |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| **Name of indicator** | **A17c Concerns and programs** |
|---|---|
| Definition | Measures the concerns and programs which are currently highest in the agenda of industries<br>CONCERNS: Malicious code, loss of privacy/confidentiality, Electronic exploits/tools, system (un)availability, Physical security, other<br>PROGRAMS: Security for web and/or ecommerce operations, Threngthening the perimeter to prevent external intrusions, centralised management of security policies and controls, secure remote access, preventing unauthorised employee access, messaging/E-mail security, other, database security. |
| Notes | - |
| Sources | Information Security Industry Survey<br>http://www.infosecuritymag.com/ |
| Countries covered | USA |
| Time series available | Periodically |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| **Name of indicator** | **A17d Security breaches** |
|---|---|
| Definition | Breaches in the previous 12 months (and their impacts)<br>(Insider breaches, outsider breaches, trends and impacts) |
| Notes | - |
| Sources | Information Security Industry Survey<br>http://www.infosecuritymag.com/ |
| Countries covered | USA |
| Time series available | Periodically |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| **Name of indicator** | **A17e E-commerce activity** |
|---|---|
| Definition | Percentage of firms conducting e-Commerce (yes/no)<br>Kinds of E-commerce conducted (B2B, B2C, Both, Only B2B, only B2C, does not anser)<br>Risks due to breaches |
| Notes | - |
| Sources | Information Security Industry Survey<br>http://www.infosecuritymag.com/ |
| Countries covered | USA |
| Time series available | Periodically |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| **Name of indicator** | **A17f Security controls** |
|---|---|
| Definition | Sorts of security tools and products used (e.g. User Ids, PW, firewalls etc) |
| Notes | - |
| Sources | Information Security Industry Survey<br>http://www.infosecuritymag.com/ |
| Countries covered | USA |
| Time series available | Periodically |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| **Name of indicator** | **A18 Computer crime - Arrests and convictions** |
|---|---|
| Definition | Prosecuted computer crime cases, arrests and convictions |
| Notes | Includes a glossary of terms and a list of press releases from recently prosecuted computer crime cases |
| Sources | Computer Crime and Intellectual Property Section (CCIPS) of the criminal division of the US department of Justice |
| Countries covered | USA |
| Time series available | Continuous update |
| eEurope relevance | 1c-x |
| Future value | Supposedly it has future value when updating findings periodically |
| Links to other indicators | - |

| Name of indicator | A19 Fixed network fraud and cellular fraud |
|---|---|
| Definition | Amounts of losses due to fixed network fraud and cellular fraud |
| Notes | - |
| Sources | Fraud and Security update; Institute for Communications Arbitration and Forensics (ICAF)- ICAF/CMA Fraud & Security SIG (Journal of) |
| Countries covered | USA |
| Time series available | Continuos updating |
| eEurope relevance | 1c-1 |
| Future value | - |
| Links to other indicators | - |

## *12.2 Review of innovative indicators under development[83]*

*Overview table*

| No. | Name of indicator | Sub-domain | eEurope code | Main Source |
|---|---|---|---|---|
| B1 | How concerned about security | Trust and Security | 1c-x | GVU-Georgia Institute of Technology |
| B2 | How concerned about security for eCommerce | Trust and Security | 1c-1<br>1c-x | GVU |
| B3 | Security a factor in on-line business | Trust and Security | 1c-1 | GVU |
| B4 | Internet privacy laws | Trust and Security | 1c-3 | GVU |
| B5 | Willing to be on-line directory | Trust and Security | 1c-x | GVU |
| B6 | Willing to use credit card on the Web | Trust and Security | 1c-1 | GVU |
| B7 | Concern about international business on-line | Trust and Security | 1c-1 | GVU |
| B8 | Which is more important | Trust and Security | 1c-1<br>1c-3 | GVU |
| B9 | Usefulness of security metrics | Trust and Security | 1c-1<br>1c-3 | GVU |
| B10 | Knowledge of information logged per page request | Trust and Security | 1c-1<br>1c-3 | GVU |
| B11 | Reasons for not registering | Trust and Security | 1c-x | GVU |
| B14 | Privacy of communications | Trust and Security | 1c-x | GVU |

[83] Innovative indicators are distinguishable from traditional indicators. They do not necessarily come from a source established as an authority in the collection of statistical information on cybercrime. They address subject matters that do not correspond to cybercrime in the traditional sense. For instance, privacy issues have important implications for the establishment of an effective and broad-based information society but are not a cybercrime in the sense that fraud is. Web defacement on the other hand might be thought of as an innovative rather than a traditional crime. Finally innovative indicators are characterised by the source given. For instance some of these indicators are derived from news reports rather than the original source.

| No. | Name of indicator | Sub-domain | eEurope code | Main Source |
|---|---|---|---|---|
| B15 | Who's worried about privacy? (study title) | Trust and Security | 1c-x | Business Week |
| B16 | 1999 PC loss study (study title) | Trust and Security | 1c-1<br>1c-x | Safeware's The Insurance Agency Inc. |
| B19 | Internet Privacy Survey (Internet users) (study title) | Trust and Security | 1c-1<br>1c-x | The Gallup Organization |
| B20 | Internet Privacy Survey (E-mail users) (study title) | Trust and Security | 1c-1<br>1c-x | The Gallup Organization |
| B21 | Behind the Numbers: Privacy and Practices on the Web (study title) | Trust and Security | 1c-x | Centre for Democracy and Technology (CDT) |
| B22 | Privacy @ Net (study title) | Trust and Security | 1c-x | Consumers International (Office for Developed and Transition Economies) |
| B23 | Shopping Online 2001-An International Comparative Study on Electronic Commerce (Study title) | Trust and Security | 1c-x | Consumers International (Office for Developed and Transition Economies) |

*Indicator descriptions in detail*

| **Name of indicator** | **B1 Security concerns of Internet users** |
|---|---|
| Definition | Level of concern about Security on the Internet as voiced by citizens, also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level.<br><br>In general, how concerned are you about security on the Internet? (e.g people reading your email, finding out what websites you visit, etc.) Keep in mind that "security" can mean privacy, confidentiality, and/or proof of identitiy for you or for someone else. |
| Notes | Methodology: the Internet presents a unique problem for surveying. At the heart of the issue is the methodology used to collect responses from individual users. Since there is no central registry of all Internet users, completing a census, where an attempt is made to contact every user of the Internet, is neither practical nor feasible financially. As such, Internet surveys attempt to answer questions about all users by selecting a subset of users to participate in the survey. This process of determining a set of users is called sampling, since only a sample of all possible users is selected.<br><br>There are two types of sampling, random and non-probabilistic. Random sampling creates a sample using a random process for selection of elements from the entire population. Thus, each element has an equal chance of being chosen to become part of the sample. To illustrate, suppose that the universe of entities consists of a hat that contains five slips of paper. A method to select elements from the hat using a random process would be to 1) shake the contents of the hat, 2) reach into the hat, and 3) pick an slip of paper with one's eyes closed. This process would ensure that each slip of paper had an equal chance of being selected. As a result, one could not claim that some slips of paper were favored over the others, causing a bias in the sample.<br><br>Given that the sample was selected using a random process, and each element had an equal chance of being selected for the sample, results obtained from measuring the sample can generalize to the entire population. This statistical affordance is why random sampling is widely used in surveys. After all, the whole purpose of a survey is to collect data on a group and have confidence that the results are representative of the entire population. Random digit dialing, also called RDD, is a form of random sampling where phone numbers are selected randomly and interviews of people are conducted over the phone.<br><br>Non-probabilistic sampling does not ensure the elements are selected in random manner. It is difficult then to guarantee that certain portions of the population were not excluded from the sample since elements do not have an equal chance of being selected. To continue with the above example, suppose that the slips of paper are colored. A non-probabilistic methodology might select only certain colors for the sample. It becomes possible that the slips of paper that were not selected differ in some way from those that were selected. This would indicate a systematic bias in the sampling methodology. Note that it is entirely possible that the colored slips that were not selected did not differ from the selected slips, but this could only be determined by examining both sets of slips. |

| | |
|---|---|
| | "Security" can mean privacy, confidentiality, and/or proof of identity |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B2 How concerned about Security for eCommerce** |
|---|---|
| Definition | Measures the level of concern about Security on the Internet by citizens, also broken down by<br>How concerned are you about security in relation to making purchases or banking over the Internet? Keep in mind that "security" can mean privacy, confidentiality, and/or proof of identitiy for you or for someone else<br>• Location (USA vs Europe)<br>• Gender<br>• Age<br>• Experience<br>• Skill level |
| Notes | Methodology: see Indicator B1<br>“Security” can mean privacy, confidentiality, and/or proof of identity |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | • 1c-1<br>• 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B3 Security a factor in on-line business** |
|---|---|
| Definition | Measures to what extent security features would be a factor at all in choosingwhether or not to do business with an Internet-based company, according to statements by Internet users. Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-1 |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B4 Demand for Internet Privacy Laws as voiced by Internet users** |
|---|---|
| 0 | Measures to what extent the Internet users express the need for new Internet privacy laws. Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level.<br>There should be new laws to protect privacy on the Internet (yes or no). |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-3 |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B5 Willingness to be listed in on-line directory** |
|---|---|
| Definition | Extent to which Internet users are willing to put their name and address in a directory for public access on the Web (e.g. the on-line equivalent of a phone company's "White Pages"). Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B6 Willingness to use credit card on the Web** |
|---|---|
| Definition | Extent to which Internet users are willing to use their credit card on the web. Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-1 |
| Future value | |
| Links to other indicators | |

| **Name of indicator** | **B7 Concern about international business on-line** |
|---|---|
| Definition | Level of concern about conducting business on-line with companies outside of one's own country, without a statement of the security procedures used. Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level. |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-1 |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B8 Preferences regarding privacy and convenience of online shopping systems** |
|---|---|
| Definition | Level of concern about privacy vs convenience by Internet users. Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level. |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | • 1c-1<br>• 1c-3 |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B9 Perceived usefulness of security metrics** |
|---|---|
| Definition | Extent to which users consider metrics indicating "how secure" a specific site is helpful or valuable.<br>Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level. |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | • 1c-1<br>• 1c-3 |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B10 Knowledge of information logged per page request** |
|---|---|
| Definition | Level of awareness of what sort of personal information can technically be collected when viewing a Web page.<br>Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level. |
| Notes | Methodology: see Indicator B1<br>Question: When you view a Web page, you issue a request to a machine that returns the page to you. To the best of your knowledge, which of the following information is technically possible to record/log about your page request? (Please check all that apply.) |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | • 1c-1<br>• 1c-3 |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B11 Reasons for notregistering at on-line sites** |
|---|---|
| Definition | Factors that cause Internet users to refrain from filling out on-line registration forms at sites, as voiced by Internet users.<br>• Takes too much time<br>• Requires me to give my name<br>• Requires me to give an email address<br>• Requires me to give my mailing address<br>• Information is not provided on how the data is going to be used<br>• Accessing the site is not worth revealing the requested information<br>• I do not trust the entity collecting the data<br>• I always register<br>• other reasons<br>Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level. |
| Notes | Methodology: see Indicator B1 |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-x |
| Future value | |
| Links to other indicators | |

| **Name of indicator** | **B14 Privacy of communications** |
|---|---|
| Definition | Measures users' assessment about the possibility of communicating over the Internet without people being able to read the content.<br>Also broken down by Location (USA vs Europe), Gender, Age, Experience, Skill level. |
| Notes | Methodology: see Indicator B1<br>Statement: I ought to be able to communicate over the Internet without people being able to read the content [yes/no] |
| Sources | GVU- Georgia Institute of Technology- 10th survey, October 1998 |
| Countries covered | All |
| Time series available | Was sixth monthly but no further survey has been done after October 1998 |
| eEurope relevance | 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B15 Lost privacy as an inevitable side effect of the Internet** |
|---|---|
| Definition | Percentage of Internet users who agree to the statement that lost privacy is an inevitable side effect of embracing the Net |
| Notes | The Fox poll consisted of interviews with a representative samples of 900 registered voters and was conducted June 7-8, 2000. |
| Sources | http://www.businessweek.com |
| Countries covered | USA |
| Time series available | not known |
| eEurope relevance | 1c-x |
| Future value | Supposedly such an indicator must be frequently updated and will have little value in 3/5/10 years time |
| Links to other indicators | - |

| **Name of indicator** | **B16 Personal Computers Damage Claims** |
|---|---|
| Definition | Total sum of personal computers damage claims at US insurance company Safeware, per year. |
| Notes | Safeware's annual loss statistics are projected from actual reported claims by the company's national client base. The company, which is a member of Assurant Group, is the largest insurer of personal computers in the United States. |
| Sources | Insurance PC Loss Study; Safeware Insurane Agency Inc.<br>http://www.cybercrimecorp.com/statistics.html |
| Countries covered | USA |
| Time series available | 1997, 1999 |
| eEurope relevance | • 1c-1<br>• 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B19 Concerns about privacy on the Internet** |
|---|---|
| Definition | Surveys the concern of US web users about privacy with relation to the Internet |
| Notes | Survey included questions on the governments' actions |
| Sources | Gallup organisation |
| Countries covered | USA |
| Time series available | - |
| eEurope relevance | • 1c-1<br>• 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B20 Concerns about privacy of e-mail communication** |
|---|---|
| Definition | Surveys the concern of US E-mail users about privacy with relation to the Internet |
| Notes | Survey included questions on the governments' actions and laws |
| Sources | Gallup organisation |
| Countries covered | USA |
| Time series available | - |
| eEurope relevance | • 1c-1<br>• 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B21 Willingness to give information over the web** |
|---|---|
| Definition | Measures the willingness to give information over the web, distinguishing the case of preservation vs non preservation of anonymity. |
| Notes | - |
| Sources | Beyond Concern: Understanding Net Users' Attitudes About Online Privacy<br>(AT&T survey) |
| Countries covered | USA |
| Time series available | - |
| eEurope relevance | 1c-x |
| Future value | - |
| Links to other indicators | - |

| **Name of indicator** | **B22 Privacy @ Net** |
|---|---|
| Definition | Analyses if the Websites collect personal information, which are optional and which compulsory. It also assesses whether companies always live up to their promises on what they shall do with the information collected.<br>• Contact information provided on the Website<br>• Cost information provided on the Website<br>• Information on security policies adopted<br>• Contract terms spelled out on the Website<br>• Personal information demanded by web traders - overall (e.g. name, address, payment card number etc.) |
| Notes | The aim is to find out whether it's possible for a consumer to browse sites and gather information without giving away information about him or herself. Consumers International also wanted to investigate a company's approach to protecting the privacy of consumers' data.<br>The shopping survey was carried out in late 1998 and early 1999, involving consumer organisations in 11 countries, whose researchers ordered a total of 151 items from sites based in 17 different countries. |
| Sources | Consumers@shopping Consumers International |
| Countries covered | Australia, Belgium , Denmark, France, Hong Kong, Japan, Netherlands, Norway, Poland, Sweden, United Kingdom, United States |
| Time series available | - |
| eEurope relevance | 1c-x |
| Future value | - |
| Links to other indicators | - |

# 13 Bibliography


| | | |
|---|---|---|
| (The French Revolution Homepage: http://members.aol.com/agentmess/frenchrev/index.html) | (1789) | *Declaration of the Rights of man and of the Citizen* |
| Council of Europe | (1950) | *European Convention of Human Rights and Fundamental Freedoms* |
| OECD | (1980) | *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* |
| US Government | (1987) | *Computer Security Act* |
| OECD | (1992) | *Guidelines for the Security of Information Systems* |
| French Government | (1995) | *Directive n. 4201/SG Sécurité des systèmes d'Information* |
| OECD | (1997) | *Guidelines for Cryptography* |
| German Government | (1997) | *Federal Act Establishing the General Conditions for Information and Communication Services- Information and Communication Act* |
| German Government | (1997) | *Act on the Protection of Personal Data Used in Teleservices- Teleservices Data Protection Act* |
| Italian Government | (1998) | *Electronic Commerce Policy Guidelines* |
| US Government | (1998) | *Presidential Decision Directive/NSC-63* |
| National Committee on Vital and Health Statistics | (1998) | *National Committee on Vital and Health Statistics Report to Secretary Shalala for the period 1996-1998* |
| European Commission | (1998) | *From User to Citizen: the Citizen and the Global Information Society (Conference documents)* |
| Douwe Korff (contractor with the European Commission) | (1998) | *Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons- Final Report* |
| European Parliament and Council | (1999) | *A Community Framework for Electronic Signatures (Directive)* |

| | | |
|---|---|---|
| European Parliament and Council | (1999) | *Action Plan on Promoting Safer Use of the Internet* |
| ISO (International Office of Standardisation) | (1999) | *Common Criteria for Information Technology Security Evaluation* |
| Dutch Government | (1999) | *The Digitale Delta "Nederland on-line"* |
| PIU (UK) | (1999) | *Encryption and Law Enforcement* |
| UK Government | (1999) | *Electronic Communications Bill* |
| UK government (department of Trade and Industry) | (1999) | *Promoting Electronic Commerce (Consultation document)* |
| German Government | (1999) | *Innovation and Jobs (Action Plan)* |
| CISI (inter-ministerial committee for the Information Society) | (1999) | *Mise en oeuvre du Programme d'action gouvernemental pour la société de l'information* |
| Prof. Ulrich Sieber of the University of Wiezburg for the European council of Tampere | (1999) | *ComCrime study* |
| European Parliament and Council | (2000) | *Directive on Electronic Commerce* |
| Council of Europe | (2000) | *Crime in Cyberspace (International convention)* |
| ESIS | (2000) | *Public strategies for the Information Society in the Member States of the European Union (Report prepared by Isabelle Chatrie and Paul Wraight, LL&A )* |
| European Commission | (2000) | *eEurope - An information Society For All (communication)* |
| European Commission | (2000) | *eEurope 2002 - An information Society For All (Action plan)* |
| European Council | (2000) | *Decision to Combat Child Pornography on the Internet* |
| Dutch Government | (2000) | *The Digitale delta: Along e-Europe* |
| Dutch Government | (2000) | *The Digitale Delta: Monitor eEurope actions* |
| Swiss Government | (2000) | *Verordnung über Dienste der elektronischen Zertifizierung (ZertDV)* |

| | | |
|---|---|---|
| UK IT Security Evaluation & Certification Scheme | (2000) | *Description of the Scheme (issue n.4)* |
| US Government | (2000) | *National Plan For Information Systems Protection* |
| US Government | (2000) | *Cyber Security Information Act* |
| National Committee on Vital and Health Statistics | (2000) | *Uniform Standards for Patient Medical Record Information, report to the Secretary of the US Department of Health and Human Services* |
| European Commission | (2001) | *Unsolicited Commercial Communications and Data Protection (Analysis)* |
| European Commission | (2001) | *eEurope 2002, Impact and priorities (communication)* |
| European Commission | (2001) | *Realising the European Union's Potential: Consolidating and Extending the Lisbon Strategy (communication)* |
| European Commission | (2001) | *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (Communication)* |
| European Commission | (2001) | *Network and Information Security: Proposal for a European Policy Research (Communication)* |
| Data Protection Working Party | (2001) | *Opinion on the Council of Europe's Draft Convention on Cyber-crime* |
| Data Protection Working Party | (2001) | *Opinion on the European Ombudsman Special Report to the European Parliament Following the Draft Recommendation to the European Commission in Complaint 713/98/IJH* |
| Data Protection Working Party | (2001) | *Recommendation 1/2001 on Employee Evaluation Data* |
| Data Protection Working Party | (2001) | *Recommendation on Certain Minimum Requirements for Collecting Personal Data on-line in the European Union* |
| Data Protection Working Party | (2001) | *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment Act 2000* |
| Data Protection Working Party | (2001) | *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act* |

| | | |
|---|---|---|
| Data Protection Working Party | (2001) | *Opinion 1/2001 on the Draft Commission Decision on Standards Contractual Clauses for the Transfer of Personal Data to Third Countries under Article 26(4) of Directive 95/46* |
| German Government | (2001) | *Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations* |
| OECD | (2001) | *Guidelines for Consumer Protection in the Context of Electronic Commerce* |
| TeleTrusT Deutchland | (2001) | *Trusted e-Commerce* |
| US Commission on National Security | (2001) | *Road map for National Security: Imperative for change* |
| US Government | (2001) | *Unique Health Identifier for Individuals – A white paper* |
| French Government | (2001) | *Projet de loi sur la société de l'information* |
| French Government | (2001) | *Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique* |