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

Benchmarking Security and Trust in Europe and the US

RAND *Europe*

Leon Cremonini and Lorenzo Valeri

Any citation requires the permission of the authors

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

ISBN: 0-8330-3458-8

Published 2003 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Email: order@rand.org

Report Version: Final

Report Preparation Date: April 2003

Classification: Report

Contract Start Date: 1st January 2001

Duration: 30 Months

Partners: empirica (Germany), Work Research Centre (Ireland), Danish Technological Institute (Denmark), Technopolis (UK), Databank Consulting (Italy), Stichting RAND Europe (Netherlands), Fachhochschule Solothurn (Switzerland), Faculty of Social Sciences, University of Ljubljana (Slovenia), ASM Market Research and Analysis Centre (Poland), Budapest University of Economic Sciences and Public Administration (Hungary), Faculty of Management of the Comenius University Bratislava (Slovakia), "Dunarea de Jos" University (Romania), Institute of Economics at the Bulgarian Academy of Sciences (Bulgaria), Estonian Institute of Economics at Tallinn Technical University (Estonia), Social Policy Unit (Sozialinnen Politicus Group) (Lithuania), Computer Science Institute of the University of Latvia (Latvia), SC&C Ltd. Statistical Consultations and Computing (Czech Republic).

Abstract

Information and network security are crucial to ensuring wide participation in the information society. There is a lack of reliable data on citizens' security and privacy concerns, the impact of these concerns on the diffusion of electronic commerce, and the amount and type of breaches suffered by organisations worldwide. This could be an impediment to the implementation of on-line government services, commerce, health care, etc., for which a safe information infrastructure is a pre-requisite. This report presents the results of two pilot surveys (for citizens and for businesses) held in 2002, which addressed respondents from the European Union, Switzerland and the United States on a number of topics, among others 'Security and Trust'. This paper, which explores how Europeans and Americans experience on-line threats and vulnerabilities, is one of the products of the EU-funded project SIBIS (Statistical Indicators Benchmarking the Information Society).

CONTENTS

1. Preface

This report represents one of the main deliverables of the SIBIS project (Statistical Indicators Benchmarking the Information Society), funded by the European Commission under the 'Information Society Technology' Programme (1998-2002). The overall goal of SIBIS is to develop and pilots indicators for monitoring progress towards the Information Society, taking account of the 'e-Europe action lines'. On this basis SIBIS focuses on nine topics of interest, i.e. Telecommunications and Access, Internet for R&D, Security and Trust, Education, Work and Skills, Social Inclusion, e-Commerce, e-Government and e- Health.

Within the SIBIS project two surveys (a General Population Survey and a Decision Makers Survey for businesses) were conducted on the nine e-Europe topics between March and May 2002. This report analyses the outcomes with respect to the topic of 'Security and Trust'. The document has two main objectives, i.e. to be a support tool for views shared by experts in the area and, at the same time, to define indicators for quantifying some of the most critical indicators related to e-government such as familiarity with it, willingness to use it, experience with its services, etc.

The report is organised in six chapters and one annex. The first three chapters are designed to give the reader an idea of the main outcomes (Executive Summary), the context (Introduction) and the indicators developed (Identification of the Indicator Framework and Hierarchy). The core of the report is the analysis of indicators, provided in Ch. 5. On the citizens' side, this chapter focuses on issues related to information security and the impact of people's concerns on the development of e-Commerce; it also measures the propensity of citizens to report violations of their on-line privacy and confidentiality and studies the possible impact of doing this anonymously. On the businesses side, this chapter analyses the incidence of security breaches and their potential consequences for private and public organisations, as well as the source – actual or perceived – of such occurrences. Ch. 6 describes where further research is needed and Ch. 7 summarises the key results illustrated throughout the report. The Annex is a methodological paper that guides the reader into the surveys and the way they were constructed.

The main audience should be policy makers, statistical offices at all levels (national, e.g. CBS, Statistisches Bundesamt, Statistics Finland etc., and supranational, e.g. Eurostat, OECD), industry leaders and researchers in the domain and those involved and interested in benchmarking the domain throughout Europe and the world. The questions and the subsequent indicators developed by SIBIS should be considered by those institutions as a valuable input for their yearly surveys. The project includes a series of workshops with such institutions in the countries represented by the SIBIS consortium. The report should also be of interest to the European Commission (in particular DG INFSO) and to government officials dealing with information security programmes.

Within SIBIS, another report (WP2) for each of the nine topics has been developed during 2001. That report was aimed at setting the scene on the topic, defining the gaps in the statistical coverage and suggesting innovative indicators to be developed through the subsequent survey. The current report, although a self-contained document, is an interim report, since a final summary version will be produced by July 2003.

SIBIS is led by Empirica (Bonn, Germany), and includes the following project partners: RAND Europe (Leiden, The Netherlands), Technopolis Ltd. (Brighton, UK), Databank

Consulting (Milan, Italy), Danish Technological Institute (Taastrup, Denmark), Work Research Centre Ltd. (Dublin, Ireland), Fachhochschule Solothurn Nordwestschweitz (Olten, Switzerland).

RAND Europe is an independent think tank that serves the public interest by improving policymaking and informing public debate. Its work is objective and multidisciplinary. Clients are European governments, institutions, and firms with a need for rigorous, impartial analysis on the hardest problems they face. This report has been peer-reviewed in accordance with RAND's quality assurance standards (see http://www.rand.org/about/standards/) and may therefore be represented as a RAND Europe product.

For more information about RAND Europe or this document, please contact:

Leon Cremonini (Associate Analyst)
E-mail: leon@rand.org

Lorenzo Valeri (Senior Analyst)
E-mail: lvaleri@rand.org

Maarten Botterman (Director of Information Society Programme)
E-mail: maarten@rand.org

RAND Europe
Newtonweg 1
2333 CP Leiden – The Netherlands
Tel. 0031 71 5245151
Fax. 0031 71 5245191
E-mail: reinfo@rand.org

2. Executive Summary

2.1 Context

Information and network security are increasingly recognised as vital elements for ensuring wide participation in the Information Society. As new business models are being developed to exploit the positive functionalities provided by these new global communication and information media, concerns about the security and privacy of information infrastructures and services may inhibit their full take-up. These concerns may hamper users' trust towards these new information and communication instruments. However, in order to tackle these concerns, it is necessary to determine who the stakeholders are: citizens, businesses and governments.

Citizens are the first class of stakeholders of the European information society. They are often at the receiving end of the public and commercial online services and tools. Consequently, it is necessary to assess and determine their perspectives and perceptions concerning online security and trust.

Businesses are the second class of stakeholders examined by SIBIS. In part businesses have similar concerns and problems as consumers with regard to security. There is, additionally, the issue of guaranteeing privacy on one hand, and wanting to benefit from micro data on customers (purchasing behaviour etc.) on the other hand. Whereas collecting such data in order to target customers better and predict market behaviour more accurately is attractive, it may backfire, as potential consumers may want to opt out.

This is where governments, the third group of stakeholders, have an explicit role to balance out interests of citizens/consumers with that of businesses. The role of governments is to balance these interests for the general good, adopting necessary regulations and trying to assure the highest degree of security for its citizens on the one hand, and avoiding putting up too high thresholds for businesses on the other.

SIBIS (Statistical Indicators Benchmarking the Information Society) developed and piloted a number of *Security and Trust* indicators, covering perceptions and experiences of citizens and businesses in Europe and the United States. Before SIBIS, data on information security issues was largely absent. By means of two pilot surveys, i.e. the GPS (General Population Survey) and the DMS (Decision Makers Survey), SIBIS tried to fill this gap. This report is intended to inform national and supranational statistical agencies, assisting them in their formulation of indicators for measuring the status and progress of the Information Society. It defines indicators for quantifying some of the most critical variables related to computer security (risk, quality of security policies and 'quality' of security breaches).

The GPS was conducted on a population of 11,832 persons aged 15 and over, living in private households, while the DMS was carried out on a population of 3,139 establishments belonging to four aggregated industry sectors in seven European Union member states (Finland, France, Germany, Greece, Italy, Spain and the United Kingdom). As a first selection, the sample on which the analyses of SIBIS generated

data are based upon answers given by those who used the Internet in the four weeks previous to the survey (for the GPS) and establishments present on-line (for the DMS survey). This procedure effectively reduced the number of actual respondents and, in fact, means that the surveys do not put the data in the context of Internet use ''maturity'' in different countries, which in turn can result in lower reliability of the data. Also, to avoid asking respondents questions about unfamiliar issues, a nested structure for asking the questions was chosen. The effect was to shorten the time needed to complete the survey. At the same time, this further limited the usefulness of the data, because only a subset of respondents provided answers to certain questions, while it would have been useful for all to respond. Without these responses, it proved difficult to get the overall picture*. Hence, it must be borne in mind that any conclusions drawn in this report are the upshot of trials (the GPS and the DMS) and, thus, a way to illustrate the use and validity of newly developed indicators*.

2.2 Main Outcomes of the Report

People are concerned about data security and privacy and these concerns effect eCommerce

Citizens' concerns over privacy and data security are strong (70% – 80%) all over Europe and in the US. These worries have an impact on B2C (Business to Consumer) e-Commerce. In fact, about two thirds of respondents are prevented from buying or banking on-line because of their concerns. However, in this respect there are clear divergences amongst countries: the Mediterranean area (Italy, France, Spain and Greece) clearly lags behind central-northern Europe (Denmark, Netherlands, Finland, Sweden, Austria, Germany) and the US. In the latter a high intensity of e-Commerce is coupled with a low impact of security concerns on people's resolution to buy or bank over the Internet; in the former, on the contrary, one can witness few people buying or banking on-line and, furthermore, they are often stopped from doing so because of their security concerns.

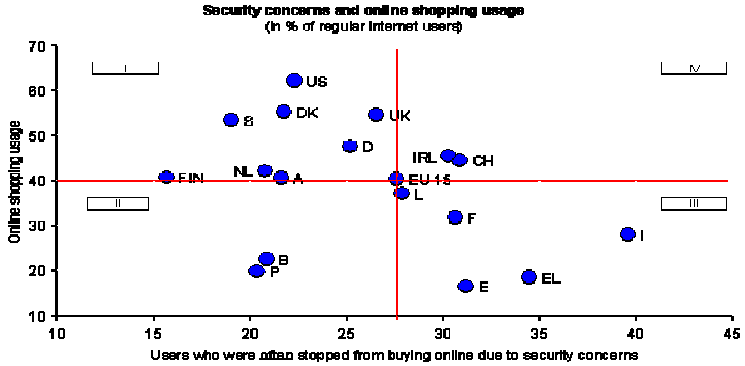


Figure 1 – Security Concerns and on-line Shopping Usage

Who buys or banks on-line knows what he's doing. What about the others?

GPS data shows that people buying or banking on-line are generally aware (74%) of security features of websites, such as the deployment of virus protection software. Not only they know such features exist, but they take them into consideration when opting (or not) for e-Commerce. However, since 'e-buyers' are a small subset of Internet users, these figures prove different when all regular Internet users are accounted for: in this case less than 20% of 'on-liners' are aware and judge security features of websites 'important'.

Reporting on-line violations is common among Internet users; being able to do so anonymously will not make the difference.

Over 80% of regular Internet users are willing to report on-line violations to a third independent party, such as an *ad hoc* public agency. Boosting this tendency even more could be a fundamental step towards the enhancement of information security infrastructures worldwide, but a truly effective way to achieve this goal is yet to be found. For instance, GPS data suggests that the opportunity of reporting anonymously has only a marginal effect on citizens' propensity to do so: amongst Internet users, merely between 4% (Netherlands) and 13% (Italy) would be more willing to report online violations if anonymity would be provide. The remaining users would report regardless[1].

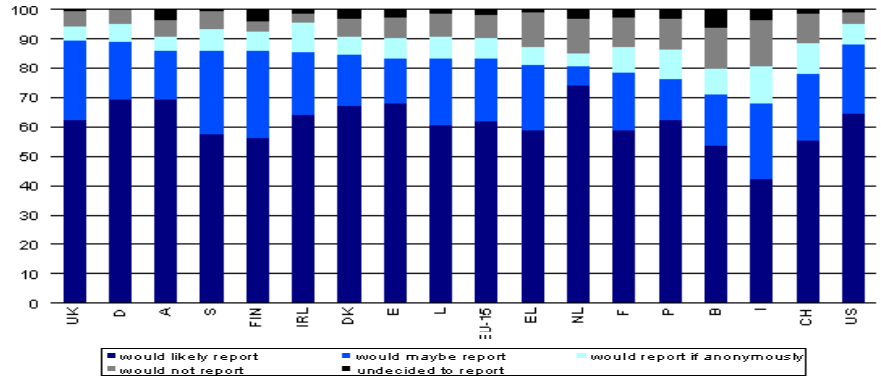


Figure 2 – Reporting of on-line Violations

Information security policies pay off: although nearly all establishments suffered computer viruses, most of the times their own information security system alerted them and severe damages were avoided

79% of European organisations have an information security policy, and 54% define it as 'formal'. DMS data shows that it pays off: with the notable exception of computer virus infections (95%), European businesses present on-line rarely suffer security breaches. Mostly, these incidents are believed to originate from hackers (41%) or internal users (29%), but seldom from customers (14%), competitors (7%) or former employees (5%). At the same time, the actual source of information on security incidents is generally internal to the establishment: most managers are alerted about the occurrence of breaches by their own information security systems (62%) or 'notice themselves' (52%). The loss of data as a source of information is uncommon (13%), as well as information provided by outsourced security services (7%). Concerning the last point, it is noteworthy that outsourcing the security management is not regarded as a chief priority by European organisations (less than half on-line businesses define it as 'high' or 'medium' information security priority), contrary to blocking unauthorised access to internal networks (over 90%), defining the security architecture (little less than 80%) and expanding the budget for enhanced security (about 85%).

In southern Europe security

The severity of security incidents is greatest in the Mediterranean countries and lowest in Finland. The DSI (Damage Severity Index), is a

1 This indicator measures the extent to which anonymity can facilitate citizens' reporting of on-line violations, but does not refer exclusively to individuals who would report only under assurance of anonymity. Thus, part of respondents might be prone to report incidents without assurance of anonymity, but nonetheless could feel facilitated in reporting incidents under conditions of anonymity.

breaches are more damaging

compound indicator[2] measuring the severity of damages suffered in the seven DMS countries. It is based on the seriousness of damages caused by different sorts of breaches (Identity theft, on-line fraud etc.). In the DSI higher numbers correspond to higher damage severity. In the DSI a country will 'score' 5, in the best 1.

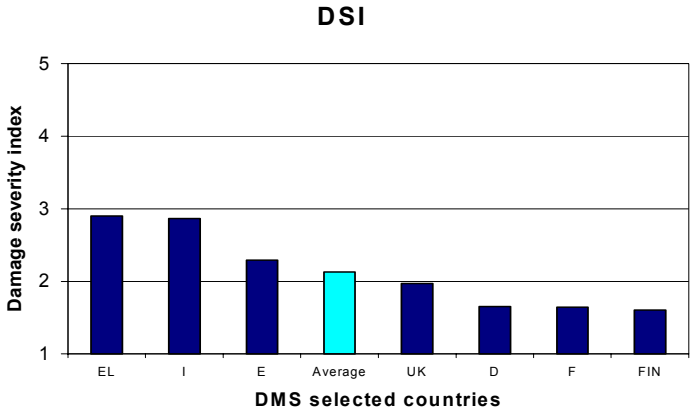


Figure 3 – Damage Severity Index

2 For the purposes of this report, a compound indicator can be interpreted as a combination of different yet related indicators. It is a method used to scale measures in order to facilitate comparisons otherwise difficult to perform. Through weighted averaging, compound indicators take care of differences in size, units etc. putting the information in a uniform and 'unitless' footing

3. Introduction

3.1 Topic Area Definition

3.1.1 Problem Description

One of the most perceptible effects of the '2002 eEurope Action Plan has been on the national and international public policy processes, since there has been a general realisation about the overall socio-economic and cultural implications of the Internet.[3] The Internet and new information and communication technologies are international by nature and, consequently, seem to be changing previous 'rules of the game'. This is particularly evident in areas such as the privacy of personal data, information security, taxation, and consumer protection. Immediate and rapid solutions are required. 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[4]. However, technology cannot provide all the answers to human-posed problems: information security is often a management issue rather than a technical problem. The answer to the dilemma is to adopt specific measures to counter those online threats and vulnerabilities.

SIBIS provides new indicators, as well as new ways to try and measure controversial variables related to information security, within the framework of eEurope. In this sense, the topic of security and trust fits in the context of the first objective of the 2002 eEurope action plan ('A Cheaper, Faster and Secure Internet'). More recently, the European Union has launched a comprehensive strategy based on the Communications on *network security*, *cyber crime* and the current and forthcoming *Data Protection Directive* regarding electronic communications. Based on the 28 January 2002 Resolution, a number if initiatives (e.g. the establishment of a cyber security task force, awareness campaigns, promotion of good practices, and improved exchange of information mechanisms) was completed by the end of 2002[5].With eEurope 2005 the European Commission proposes policy and supplementary statistical indicators, partly already covered by SIBIS[6].

Although some attempts have been made to assess issues of information security (such as occurrence of breaches, their seriousness etc.[7]), these were not specifically focused on the European Union. In addition, these surveys were conducted on-line, thus excluding all those persons with limited Internet access (for example because they could not access Internet from home). Notwithstanding time constraints and methodological limitations (such as the limited sample of respondents due to a necessary selection),

3 See for example European Commission (2002), eEurope 2002 - An Information Society For All (Action plan), Council of Europe (2000), Crime in Cyberspace (International convention), or the many Opinions and Recommendations of the Data Protection Working Party, and the many national legislative acts on these issues. The OECD is also actively involved in these matters through the creation of guidelines and regulatory papers, such as OECD (2002), Guidelines for Information and Network Security: Towards a Culture of Security OECD (1997) Guidelines for Cryptography, OECD (1992), Guidelines for the Security of Information Systems OECD (1980), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 .

4 Cf. for example WebWatch (2002), *A Matter of Trust: What Users Want form Websites*, available at http://www.privacyexchange.org; Consumers' International, *Shop On-line 2001: An International Comparative Study of Electronic Commerce*, September 2001; etc.

5 eEurope 2005: An information society for all, pp. 15-16 . On this aspect see eEurope 2005 Key Figures for Benchmarking EU 15, by Databank Consulting (SIBIS WP 4 – D. 4.3.3)

6 Ibid.

7 See for example the GVU user surveys, available at http://www.gvu.gatech.edu/user_surveys/, which provide information on the growth and trends in Internet usage.

SIBIS represents a first attempt in this direction, specifically targeting EU, US and Swiss citizens and organisations through telephone-assisted interviews.

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. For example, it is acknowledged that a lack of trust and confidence in services provided electronically is a significant barrier to the development of e-Government[8]; SIBIS evidence (cf. Chapter 5 below) shows that, more often than not, electronic commerce is stopped by security and privacy concerns. The *eEurope 2005 Action Plan* stresses the importance of on-line security and trust for IS developments; etc. If individuals are suspicious, and, therefore, reluctant to send the identifying or financial information required to complete transactions over the Internet, the fraction of commercial and societal activities that can benefit from transition to the electronic medium will be significantly restricted. Consequently, 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, hence its pivotal policy implications.

From the viewpoint of the commercial sector, the issues in this area are different. One of the main benefits perceived by firms from the Information Society is the opportunity to use information about consumers to target their marketing strategies, understand their customer bases, devise new products, and improve the efficiency of their internal operations. If, for example, access to comprehensive information on individual preferences and purchasing habits allows a firm to precisely target its marketing campaign, it may be possible for the company to generate the same level of sales for a fraction of the cost of a 'traditional' broad based marketing effort. At the same time, a company's secure information infrastructure is crucial for consumers to approach the firm in the first place, and for the establishment to be protected against possible external breaches. The fact that most of European organisations adopt an information security policy suggests that this is taken into thorough account (Cf. Chapter 5.2.3, below)

Acknowledging that security and trust are important issues in the development of the e-economy and the Information Society, *e*Europe documents state that 'the market should, as far as possible, be left to determine the adequate amount of security for user needs.' Without good performance indicators in this area, firms, security suppliers, and consumers will be unable to make informed decisions about the current or desired level of security and privacy.

8 See for example, Progressing the Information Society: the role of government, Report on the JANUS Workshop, Brussels, 17 February 2003, p.39; Cf. also Graafland-Essers, I. & Ettedgui. E. (2003), Benchmarking e-Government in the Information Society in Europe and the US, SIBIS Topic Report n. 8

3.1.2 Framework for Assessing the Area

Although European policy on the Information Society is often framed in terms of promoting 'trust and confidence', 'trust' does not seem to be a viable indicator for the assessment of the Information Society because of its multidimensional nature. Trust has many definitions and defining it in a measurable way is not possible.

The Information Security literature characterises 'trust' as a particular functionality provided by Public Key Infrastructures (PKI), allowing two or more actors to authenticate one another and establish a situation where neither party can repudiate commitments undertaken electronically. Instead, in the more general context of the Information Society and electronic commerce, trust refers to 'softer' issues about on-line marketing, quality control, business processes and customer relationship management.[9]

According to an article published in *The Journal of Management* in 1991[10], 'trust' is the willingness to rely on an exchange partner, i.e. the expectation that a merchant's word is reliable and that the seller will not take advantage of the consumer's vulnerability. In this context, trust is not related just to technical arrangements but arises from a mix of factors (legal, social, cultural, individual etc.), which are hard to quantify in an Information Society environment. It becomes crucial, then, to assess how trust is established in on-line environments.

Sapient, a global e-commerce consultancy firm, suggested that trust in the context of electronic commerce should involve three components, i.e. seals of approval (symbols informing users on an ensured level of security), brand and fulfilment (a promise to deliver specific attributes), and navigation, presentation and technology (involving the use of technological solutions that imply quality and professionalism).[11]

According to the survey *E-Commerce and Consumer Protection*[12], conducted in 2000 by the National Consumer Council, users' difficulty in trusting e-Commerce operations is not only due to concerns over data security, but also to the lack of regulation (national and international) and the difficulty in assessing a merchant's 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 on-line, either because they feel it is not attractive enough, or they see no prospect of gaining on-line access; others recognise that the Internet and on-line shopping have limitations.[13]

9 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).

10 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 Theory of Relationship Marketing', The Journal of Marketing, vol. 58 no. (July-September 1994), pp.23-34a and Donna Hoffman, Thomas Novak and Marcos Peralta, 'Building Consumer Trust On-line', Communications of the ACM, vol. 42 no. 2 (April 1999), pp. 81-84

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

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

13 Ibid.

Similar conclusions were reached in a survey conducted by Consumer International,[14] according to which trust in electronic commerce is still limited among Internet users because of concerns related to transaction costs or on the site's location and uncertainty about the overall terms and conditions of electronic transactions,[15] and a US-based survey held in April 2002 stressed that

> Users want to know who runs the site, how to reach those people if there's a problem, to find its privacy policy and how the site deals with mistakes, whether informational or transactional. For example, 80 percent of respondents say it is very important to be able to trust the information on a web site — the same percentage that say that it is very important that a site be easy to navigate.[16]

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.[17]

The literature and the surveys mentioned above confirm that building trust in the Information Society does not centre only on security but relies on various factors of difficult quantification, thus undermining the creation of a single, measurable benchmark (i.e. *representative*, *useful* and *agreed*) measuring trust[18].

2.1.3. Identification of Stakeholders and their Interactions

Individual consumers stand out as one of the most important stakeholders in this area. Important data from their perspective include both their beliefs about the level of privacy and security protection that is desirable, and at the same time, their perception of the current level of protection provided by procedural, legal, and technological mechanisms. In addition, a significant number of organisations and coalitions that represent various aspects of consumer interests and concerns are actively involved in this area. Concomitantly, commercial firms in all business sectors – from purely Internet firms to the most traditional 'old economy' companies – have an important interest in this topic. While the interests of firms and consumers often coincide in the area of security – since both groups gain from prevention of fraud or ICT mediated theft – their interests often diverge in the area of personal privacy and data usage. While firms are concerned about how these issues affect individuals' purchasing and consumption patterns, they also have legitimate concerns about how restrictions on the use of databases, information collection, and other ICT tools might affect their business and limit the economic benefit of the Information Society. A subset of firms, focusing on

14 CI is the federation of consumers' organisations dedicated to the protection and promotion of consumers' interests worldwide.
15 Consumers' International, Shop On-line 2001: An International Comparative Study of Electronic Commerce, September 2001 available at http://www.consumersinternational.org/CI_Should_I_buy.pdf
16 WebWatch (2002), *A Matter of Trust: What Users Want form Websites*, available at http://www.privacyexchange.org
17 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
18 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, Ph.D. Dissertation completed at the Department of Computer Science and Mathematics, University of Stirling, April 1994.

technologies such as encryption, smart cards, biometrics, or other protections, have shaped their business strategies around producing technological answers to these concerns. Regulators and policy-makers seek to balance these sets of competing interests in this area for the overall benefit of society.

Moreover, although citizens, governments and businesses as a whole appreciate security and are both receivers and providers of security, each one has a specific individual perspective on this matter based on its particular operational objectives. 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.

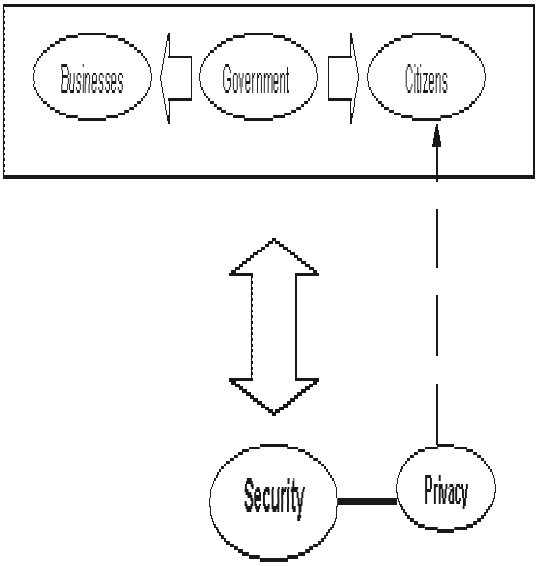


Figure 4 – Stakeholders and their Interactions

Figure 4 synthesises the stakeholders' relationships: governments, businesses and citizens are all providers and receivers of security. At the same time, privacy and security are linked, although there can be no direct causal relationship between the two, and the most sensitive to the issue of privacy are individual citizens. Finally, because the government expresses an interest for the well-being of society as a whole (aimed at the public good), it incorporates the interests and needs of business and citizens as part of its overall approach to security and privacy issues.

3.2 Overview of the Report

The next chapters of the report will mainly elaborate on the findings of the SIBIS project.

Chapter 3 will briefly summarise the indicator framework and hierarchy, underlining the list of indicators as a whole and their inter-relationships. As has been said, three main security domains were envisaged, i.e. on-line malicious activities, prevention of on-line malicious activities and downtime and on-line interaction facilitators. These will shortly be recalled, as the relevant framework for the analysis of data.

Chapter 4 describes, validates and analyses the outcomes of the citizens' survey (GPS) and the businesses' survey (DMS) and presents an example of a possible 'compound indicator' based on the DMS findings.

Chapter 5 describes which parts of analysis are still open for further developments in future surveys and indicator development studies in the area.

Chapter 6 gives the conclusions of this Topic report on Security and Trust.

The Annex provides the GPS and DMS questionnaires and a methodology paper on the surveys.

4. Identification of the Indicator Framework and Hierarchy

As discussed in the previous chapter, stakeholders in the area of information security and trust are governments, citizens and businesses. However, due to the impossibility of creating a useful, agreed and representative benchmark for 'trust', indicators have been developed specifically for the area of security. To address these issues, it is necessary to concentrate on three main domains directly relevant to security functionalities, namely *on-line malicious activities*, *prevention of on-line malicious activities and downtime* and *on-line interaction facilitators (seals and Web-based quality certificates)*. These can be measured by various indicators developed within SIBIS both through the Businesses Survey and General Population Survey.

Although there are a number of existing indicators measuring on-line malicious activities, they are difficult to define. For example, the *Convention on Cyber-crime* of the Council of Europe[19] aims at harmonising substantive and procedural legislative measures in the area of cyber-crime. The convention is expected to influence the development of national and European-wide legislation and perhaps also global legislation.[20] The convention refers to criminal activities and behaviour that may relate to the activities of many units of analysis.

However, the Convention on Cyber-crime does not cover all 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).[21]

Notwithstanding the terms of reference provided by these legal instruments, it is often the case that on-line malicious activities cannot always be defined as such. A possible solution would be to classify malicious activities as 'attacks'. For example, 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.[22]

19 The final text is available at http://conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm
20 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
21 For more information see World Intellectual Property Organisation (WIPO), 'Primer on Electronic Commerce and Intellectual Property' May 2002 available at http://e-Commerce.wipo.int/primer/index.html
22 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

Prevention of on-line malicious activities and downtime represents the other side of the equation. Measuring this aspect in parallel with the former is important to have an overview of the awareness in this area, and can influence policy-making. Indicators referring to this domain 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 on-line activities.[23] Although there are already some standardised indicators available (many public and private institutions collect data about software and hardware security expenditures), nevertheless there is a general lack of detailed data about investments or how public and private institutions manage their information security.

Seals are recognised standards certified by an auditing process involving checks on security and privacy provisions. In this aspect, they can be defined as on-line interaction facilitators. During the last few years, there has been a proliferation of these initiatives, both in the United States and in Europe, launched by private and public sector bodies[24]. Table 1 provides a list of relevant indicators, distinguishing between those that were developed in SIBIS and existing ones.

Table 1 - Overview of SIBIS indicators and relevant existing indicators

N.	Indicator Name[25]	On-line Malicious Activities	Prevention of On-line Malicious Activities	On-line Interaction Facilitators	Existing indicators of relevance for SIBIS[26]	New SIBIS Indicators[27]	Compound indicators
1.	Security breaches occurred in the organisation	X				X	
2.	Type and relevance of breaches suffered	X				X	
3.	Supposed origin of breaches	X				X	
4.	Concern regarding on-line security		X			X	
5.	Source of information on occurred breaches		X			X	
6.	Presence of security policies		X			X	
7.	Sort of information security policy		X			X	
8.	Information security priorities		X			X	

23 Security measures both against malicious activities and unplanned downtime or service delivery breakdowns.
24 A sample list may include 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), FEDMA (Federation , f European Direct Marketing) Mark, Q-Web (Italy), TrustE (USA), Web-Trade Code of , onduct (US), Webtrader (Italy), Webtrust (Italy), Which? Webtrader (UK)
25 Information in the annex of the present document
26 From published sources
27 Developed within the project

N.	Indicator Name[25]	On-line Malicious Activities	Prevention of On-line Malicious Activities	On-line Interaction Facilitators	Existing indicators of relevance for SIBIS[26]	New SIBIS Indicators[27]	Compound indicators
9.	Barriers to information security		X			X	
10.	Tools of information security		X			X	
11.	Awareness of security features of websites			X		X	
12.	Effects of Security concerns on on-line shopping behaviour			X		X	
13.	Propensity to report incidents of on-line violations without assurance of anonymity			X		X	
14.	Propensity to report incidents of on-line violations under assurance of anonymity			X		X	
15.	Importance of security features of websites on consumers' propensity to shop on-line			X		X	
16.	Internet users encountering problems				X		
17.	Computer ownerships (EUROBAROMETER 2001)				X		
18.	Financial losses due to computer breaches				X		
19.	DSI		X				X

From what has been said above, it appears that the area of information security is composed of the units of analyses (governments, industry, individuals) and the three domains of security (on-line malicious activities, prevention of on-line malicious activities, on-line interaction facilitators[28]). So much for the description of the framework itself, now we move on to illustrate how indicators developed and piloted in SIBIS fit in this framework.

28 These include seals and web-based quality certificates (i.e. recognised standards certified by an auditing process involving checks on security and privacy provisions). During the last 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 may include 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-, aerket (Denmark), FEDMA (Federation of European Direct Marketing) Mark, Q-Web (Italy), TrustE (USA), Web-, trade Code of Conduct (US), Webtrader (Italy), Webtrust (Italy),. The brand was not considered in this report as a facilitator. Arguably, it might be a significant factor in on-line trust and concerns, but is not accounted for in the results and (therefore) in the analysis.

On the one hand, although the units of analysis as a whole require security, each one has a specific individual perspective on this matter based on its particular operational objectives; on the other hand, it is not possible to combine into a single benchmark the three envisaged security domains, maintaining it at the same time representative, useful and agreed (i.e. maintaining it a benchmark).

On-line malicious activities, prevention of on-line malicious activities and downtime, and seals/web-based quality certificates refer to three different phenomena. This differentiation could be overcome through their conversion into financial measures. This would require financially quantifying the impact of on-line malicious activities or attacks. Although some surveys (see above and WP 2) have attempted to do so, they 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.[29]

The separation of 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 on-line 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 cyber-crime, network intrusions, on-line 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. On-line malicious activities, however, are just one aspect of security. Their negative implications may be prevented through appropriate technical and managerial security 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 on-line malicious activities. This state of affairs, which will be registered by the relevant benchmarks, may lead to a readjustment of policies.

29 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.

5. Analysis of Data

5.1 Analysis of Indicators for Citizens and Society

This section gives an insight into the major trends and issues emerging from the General Population Survey, conducted within SIBIS in April/May 2002. The survey was conducted in 15 European Union member states as well as Switzerland and the United States. It focuses on three key aspects for the security of information and network systems where citizens are perceived to be actively involved

1. Security and privacy concerns;
2. Effects of these concerns and the role of security features of websites on on-line shopping;
3. Citizens' propensity to report on-line violations.

As mentioned in the introduction to this report, the GPS involved a total of 11,832 individuals, spread over 15 countries. Also, as a first selection, only regular Internet users were addressed, at times limiting the number of respondents per country. Hence, although each of the outcomes is a picture purporting to be useful for the sharing of views on what needs to be done in order to reduce risk in on-line environments, in fact SIBIS does not intend to give specific policy recommendations based on its findings. Rather, it should set a good example for national and supranational statistical efforts ahead.

5.1.1 Security and Privacy Concerns

The SIBIS data shows that European and US citizens are strongly concerned both about privacy and data security, with a slightly higher concern for the former than the latter. In the United Kingdom, Republic of Ireland and the United States, as opposed to continental Europe, 88% of citizens feel strongly or somewhat concerned about privacy and roughly 78% about data security. Whether this is caused by a higher amount of negative experiences, more trust in the functioning of society-at-large or the level of awareness is not yet clear.

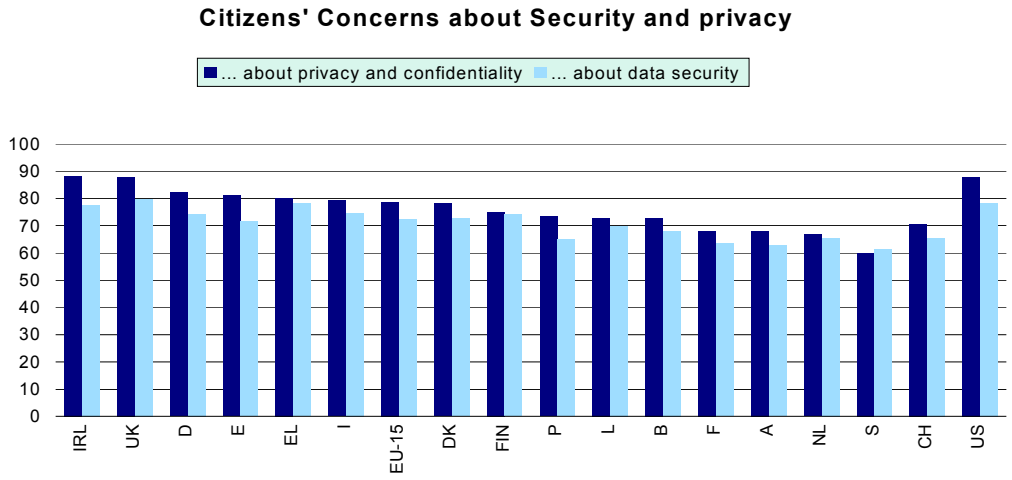


Figure 5 – Concerns regarding data security, privacy and confidentiality
Source: SIBIS, GPS 2002, weighted by EU15 population (N=5944), citizens who used the Internet in the last four weeks

5.1.2 Developing On-line shopping

The success of B2C (Business to Consumer) e-Commerce depends on several factors ranging from the prompt delivery of the ordered service or goods to the possibility of rapid redressing of disputes between customers and merchants. Another important factor is the perception of security and privacy of customers when they provide the merchant with their own personal financial details. Concerns in these specific domains might have a significant impact on individuals' propensity to shop on-line.

SIBIS surveyed concerned individuals on how often their concerns would stop them from buying goods and services over the Internet. Amongst those, about one third declared never to be stopped, but the remaining two thirds stated that security and privacy concerns often or sometimes would in fact prevent them from shopping on-line. Although it is presumable that non-concerned individuals are also not stopped from buying on-line due to their (non existing) concerns, any assumptions on their behaviour would result in mere speculations, since those persons were not addressed. Nevertheless, it is possible to take the whole population as a sample in order to assess the effective percentage of persons stopped or not from buying on-line. In this case, the relative number of individuals whose on-line shopping behaviour is negatively affected by security and privacy concerns will result in lower figures.

Figure 6 is a stacked bar chart showing the percentage of individuals who are often or sometimes stopped from acquiring goods and services over the Internet. It also reports those individuals who are not stopped from these concerns as well as the non-concerned. In Italy and the United States, about 60% of surveyed individuals do not engage on electronic commerce transactions due to concerns about their security and privacy. This percentage drops to less than 40% in Belgium and the Netherlands.

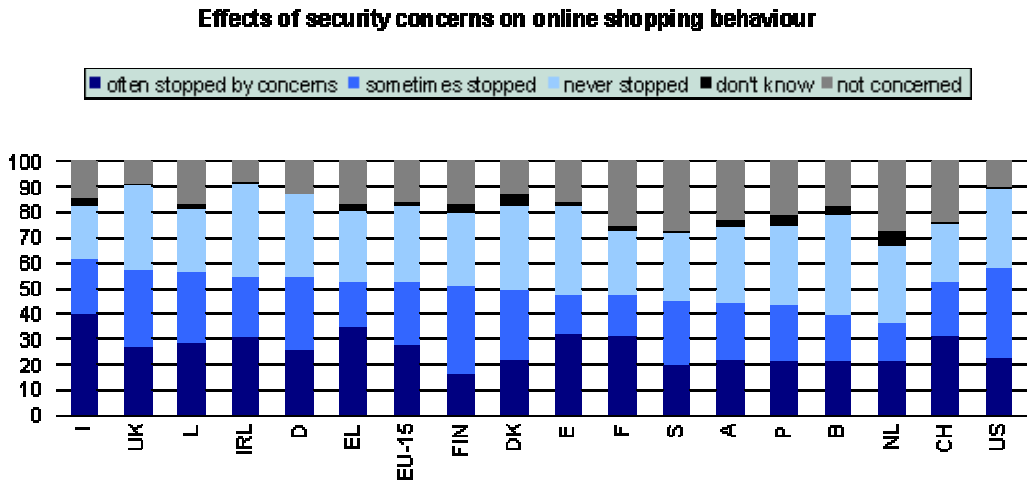


Figure 6 – Effects of security concerns on eCommerce
Source: SIBIS, GPS 2002, weighted by EU15 population (N=5944), citizens who used the Internet in the last four weeks

Moreover, it is interesting to compare 'on-line shopping usage' and the effects of security and privacy concerns on this. SIBIS clearly corroborates the idea that the intensity of Internet usage is reflected on the diffusion of electronic commerce.[30] We can imagine four possible situations regarding on-line shopping, specifically:

- A country where on-line shopping is common (high on-line shopping usage) and where the impact of security and privacy concerns is weak;
- A country where on-line shopping is uncommon (low on-line shopping usage) and where the impact of security and privacy concerns is strong;
- A country where on-line shopping is uncommon (low on-line shopping usage) and where the impact of security and privacy concerns is weak;
- A country where on-line shopping is common (high on-line shopping usage) and where the impact of security and privacy concerns is strong.

SIBIS data (as presented in Figure 7) suggests a split between 'front- runners', i.e. those countries where on-line shopping usage is high and the impact of security concerns is relatively low (quadrant I) and the 'laggards', where on-line shopping usage is low and the impact of security concerns is strong (quadrant III). As can be seen, Nordic countries, the US, the UK, Austria and Germany appear as front-runners, while all Mediterranean countries (France, Italy, Spain and Greece) are the laggards.

[30] On this aspect, cf. Databank Consulting (2003), *Benchmarking e-Commerce in the Information Society in Europe and the US*, SIBIS topic report n. 7, which deals extensively with the issue.

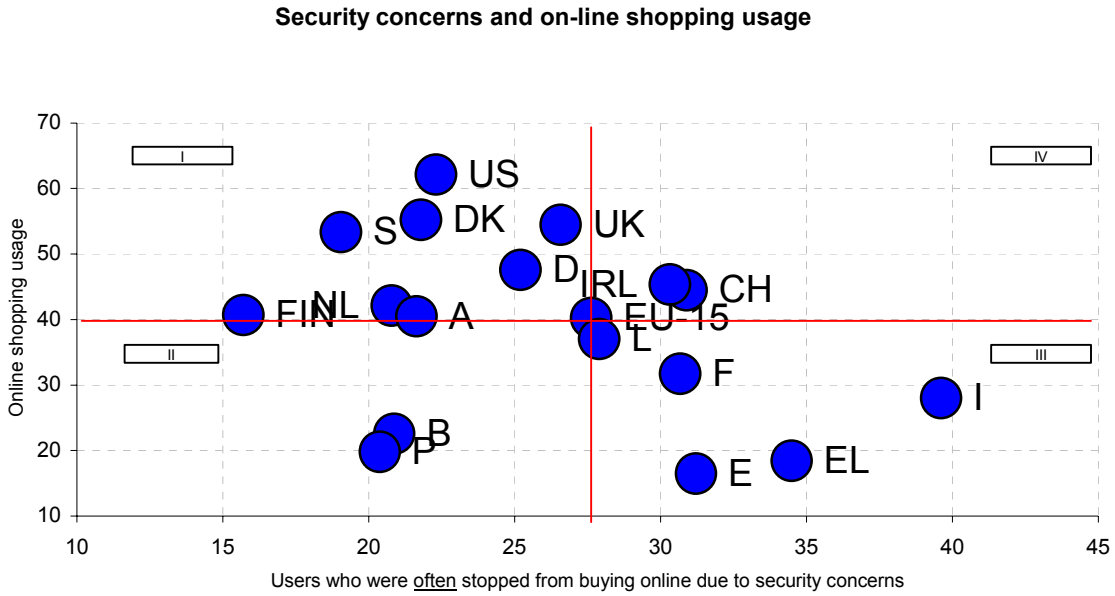
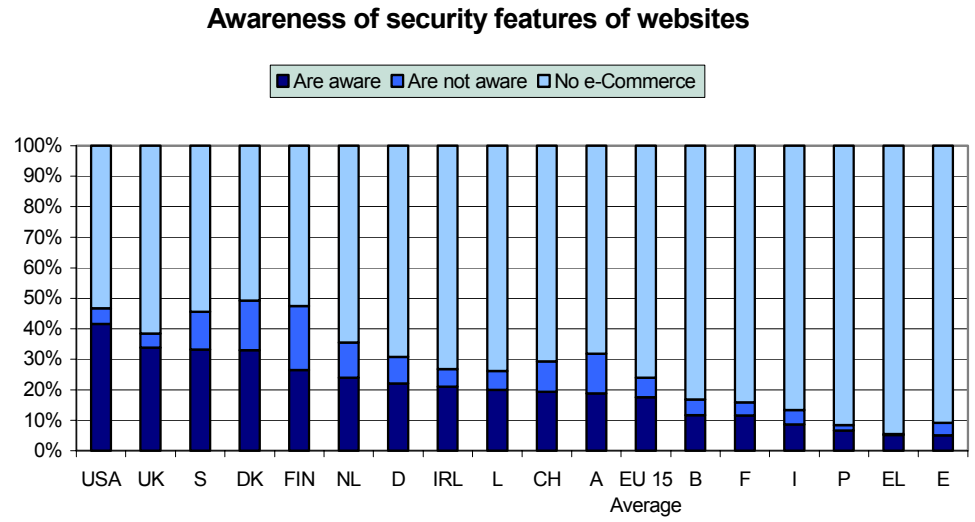


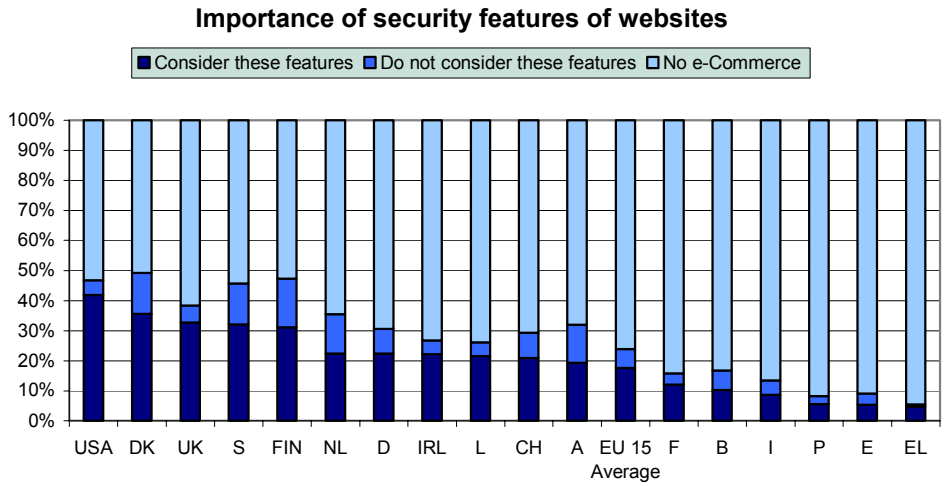
Figure 7 – Security concerns and on-line shopping
Source: SIBIS, GPS 2002, weighted by EU15 population (N=5944), citizens who used the Internet in the last four weeks

Although people are deterred from buying on-line, security features of websites such as the deployment of virus protection software, might be a way to redress these concerns. SIBIS tackles the problem under two different but complementary perspectives: *awareness* and *importance* of security features of websites.

Awareness of security features of websites is the mere knowledge of their existence; the indicator on importance, instead, measures how often users actually take these features into account when buying or banking on-line. On average, 74% of EU citizens shopping and banking on-line are aware of security features and consider them 'important'. However, the picture is quite different with regards to the overall population. In Europe, only a minority is in fact aware of these features (see Figures 8 and 9).

Data show then a two-faced picture. Persons who carry out e-Commerce are indeed aware of security features of websites; moreover, they are not just aware that these features exist, but usually keep them in consideration when they buy or bank on-line. Yet, as also outlined in the previous paragraph, at this day electronic commerce represents no more than a niche for most national economies.





Figures 8 and 9 – Awareness and importance of security features of Websites
Source: SIBIS, GPS 2002, weighted by EU15 population (N=6908), citizens who used the Internet in the last four weeks or, if not, at least once in the last 12 months

5.1.3 Reporting of on-line violations and the role of anonymity

The implementation and deployment of protective measures can encourage citizens to trust Internet-based transactions with businesses or the government . Sharing information on on-line vulnerabilities, threats and incidents is acknowledged as a key ingredient to an effective implementation of such protective measures.[31] Particularly for

31 On information sharing and early warning see DDSI, Information Sharing Roadmap and Final Report of a Workshop held in Brussels 17-18 January 2002 on 'Warning and Information Sharing', also available at http://ewis.jrc.it You should reference to the final roadmap of DDSI that was presented at the final conference that you attended…this information is available on the share drive.

viruses, but also with other kinds of problems an early warning from users can help other users worldwide to take measures to shield themselves.

SIBIS developed an indicator on citizens' willingness to report on-line violations of security, privacy and confidentiality in the 15 surveyed countries. Although data show a high preparedness to do this in all countries (only in Italy the percentage of users likely to report is just below 70%), the ability to report anonymously has no significant effect on the overall propensity to report. Further research will be needed to examine whether willingness to report violations and the impact of anonymity varies for different kinds of intrusions (viruses, unauthorised access &c).

Chart 10 shows the willingness to report violations of one's on-line security, privacy and confidentiality to a third independent party, for example a public agency created for this task, and highlights the difference induced by the option of reporting anonymously. As can be seen, the latter figure spans between 4% in the Netherlands and 13% in Italy. However, although data suggests that for certain persons it would be easier to report anonymously, since SIBIS addressed also those who would report anyhow, only a subset of this small group would in fact report *only* under assurance of anonymity – and this subset cannot be quantified based on the survey's information. Hence, figure 10 shows that European and US Internet users are willing to report on-line violations and anonymity would hardly make a difference.

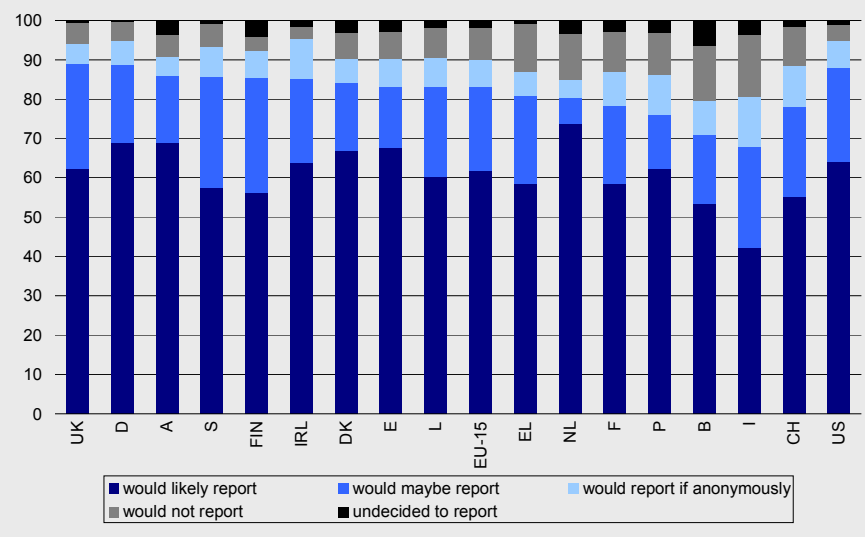


Figure 10 – Reporting of on-line violations
Source: SIBIS, GPS 2002, weighted by EU15 population (N=5,944), citizens who used the Internet in the last four weeks

5.2 Analysis of Indicators for Businesses

This section analyses the outcomes of the Decision Makers Survey, conducted in May 2002. The DMS was conducted in 7 EU states and included over 3,139 interviews in all. The next pages will expand on issues relating to information security breaches and

actions taken to prevent them. Because of a very limited number of respondents, the DMS gives simply a first snapshot of some major trends in European establishments.

5.2.1 Security breaches and their consequences

SIBIS data shows that 27.5% of organisations in the seven surveyed countries are affected by security breaches, i.e. unauthorised use and attacks to information infrastructures. However, before SIBIS, there was little data available on different kinds of information security breaches being experienced by European organisations. Although it is often suggested that hacking or dedicated high scale network intrusion are businesses' chief concerns, SIBIS found that computer virus infections (a program that can 'infect' other programs by modifying them to include a, possibly evolved, copy of itself[32]) are the most frequent type of security breach experienced, with the overwhelming majority of attacked organisations reporting to have been affected by them. The number of other security breaches reported, such as unauthorised access to their networks[33] or identity theft[34] was fairly low. Since a categorisation by country for this aspect does not show any relevant feature, it is not deemed necessary here. Figure 11 shows that, on average among the seven surveyed countries, over 90% of establishments that had been attacked, had in fact suffered viruses.

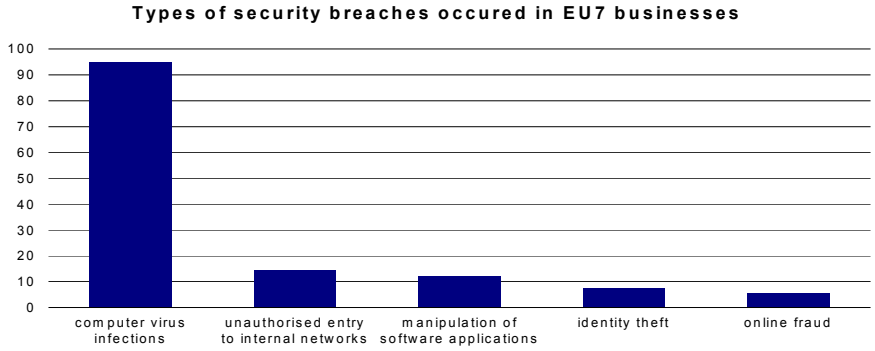


Figure 11 – Types of security breaches suffered by European organisations
Source: SIBIS, DMS 2002, weighted by Employment (N=514), Businesses with online presence, that were affected by security breaches in the last 12 months

In addition, the consequences of this sort of breaches were often severe: companies suffered substantial ('very' or 'rather') consequences in 41% of the times. Interestingly, however, under this respect national patterns do play a role. As the chart below shows[35], Europe is split between south and north, with Italy and Spain suffering 'rather' to 'very' substantial consequences in more than half of the cases (60% Spain and 55% Italy), and the other surveyed countries below average (United Kingdom 40%, France 38%, Finland 32% and Germany 27%).

32 See Security and Trust, Indicator Handbook, SIBIS WP 6, p. 6
33 Unauthorised entry is managing to access to networks without authorisation. Access is simply being able to get to what you need. Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an on-line service provider such as America On-line, in Security and Trust, Indicator Handbook, SIBIS WP 6, p. 6
34 Identity theft is a crime in which an impostor obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else, in Security and Trust, Indicator Handbook, SIBIS WP 6, p. 6
35 Because of the extremely limited number of respondents in Greece, figures relative to this country are not in the least significant and, thus, cannot be presented as part of the picture.

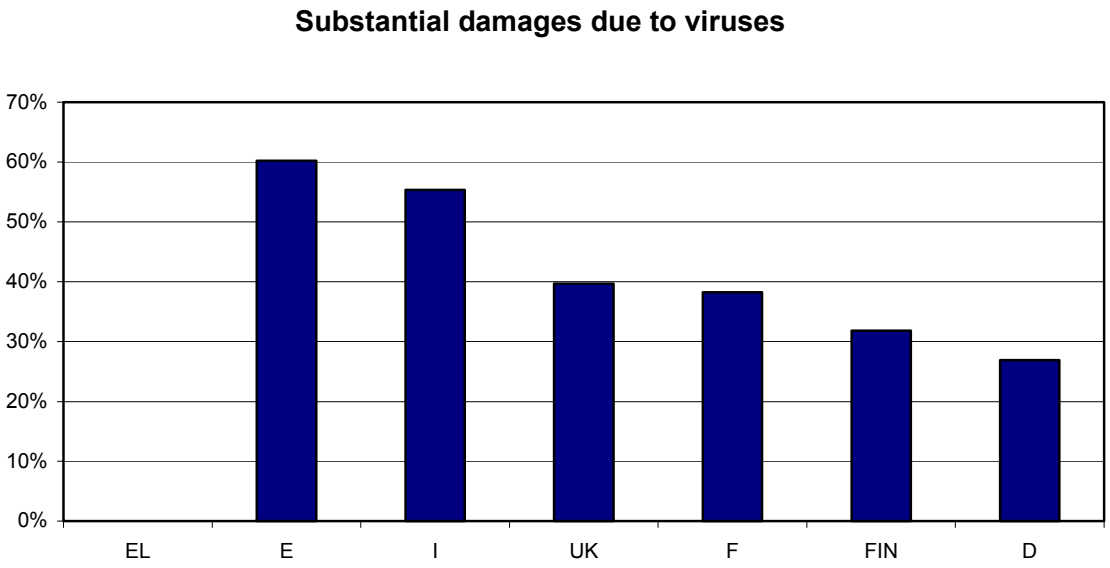


Figure 12 – Substantial consequences of virus infections in European organisations
Source: SIBIS, DMS 2002, weighted by Employment (N=484), Businesses with online presence, that were affected by computer viruses the last 12 months

5.2.2 Breaches' origin: perceptions and warning

Security breaches are the consequence of somebody's action. Victims of security breaches have their own beliefs on from where they might originate, and have different sources of information. Two indicators have been piloted in the DMS to describe these aspects, i.e. the supposed 'origin of breaches' and the 'source of alert'.

As regards the origin of information security breaches, between 30% and 40% of organisations believe they originate from computer hackers, followed shortly by insiders. However, In Greece and France hackers are perceived as the major cause of breaches in about 60% of cases (58% and 65% respectively), in Italy customers are deemed responsible for breaches more frequently than insiders (although the difference is only 5%) and in Finland internal users surpass hackers by 10%. Data do not show any national pattern (differently for example with reference to e-Commerce and the impact of security and privacy concerns), although the fact that Greece, with the lowest Internet penetration, shows internal users as the least supposed origin of breaches, and Finland, with the highest Internet penetration, conversely shows internal users as the highest supposed origin of breaches might be noteworthy.

Overall, the most significant feature is that management typically believes breaches to be caused by external hackers or internal users, but rarely by customers or competitors. Fig 13 portrays this information.

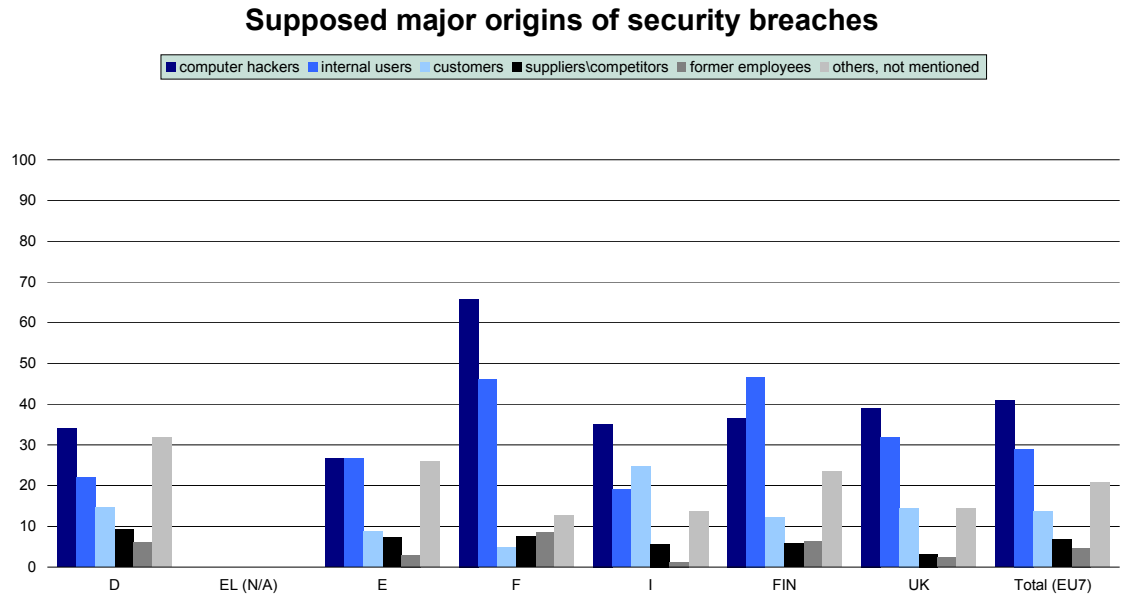


Figure 13 – Origin of security breaches suffered b y European organisations
Source: SIBIS, DMS 2002, weighted by Employment (N=514) Businesses with online presence, that were affected by security breaches in the last 12 months.

At the same time, SIBIS data suggests that European establishments still need to 'look after themselves': Information about security breaches will rarely be provided by outsourced security services (7%) or by customers (9%). Managers are more likely to learn about such incidents through internal information security systems (60%) or by themselves (50%). On the positive side, however, being alerted by loss or damage of data is relatively uncommon (13%), suggesting that, more often than not, security incidents are detected before they can trigger serious effects.

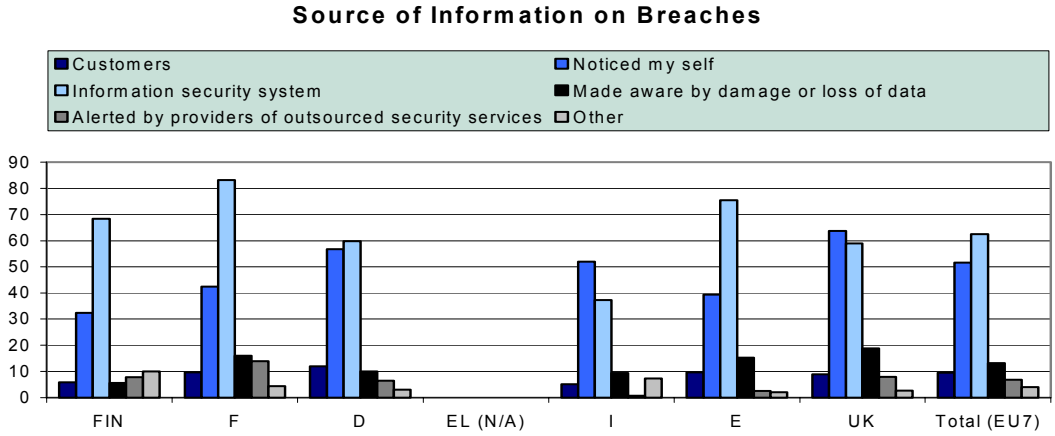


Figure 14 – Origin if security breaches suffered by European organisations;
Source: SIBIS, DMS 2002, weighted by Employment (N=514) Businesses with online presence, that were affected by security breaches in the last 12 months.

5.2.3 Pre-emptive actions: information security policies in European organisations

For the purpose of this report an information security policy is defined as a measure taken to protect information systems against unauthorised use and attacks[36]. 79% of European organisations adopt an information security policy to protect themselves against breaches. Finland is the country with the highest percentage (84%) while, , the United Kingdom scores lowest (78%) However, in fact these differences are not significant. In about 80% of the cases companies adopt some for of information security policy, whether formal, i.e. stated as a company's official policy, (54%), informal (21%) or not specified (3%). The fact that, with the exception of virus infections, the number of breaches is fairly low suggests that implementing a security policy pays off after all; on the other hand, the overwhelming presence of computer virus incidents (above 90% in European establishments), suggests that policies should be oriented according to the need. Further action, for example in terms of training and awareness raising, could be considered.

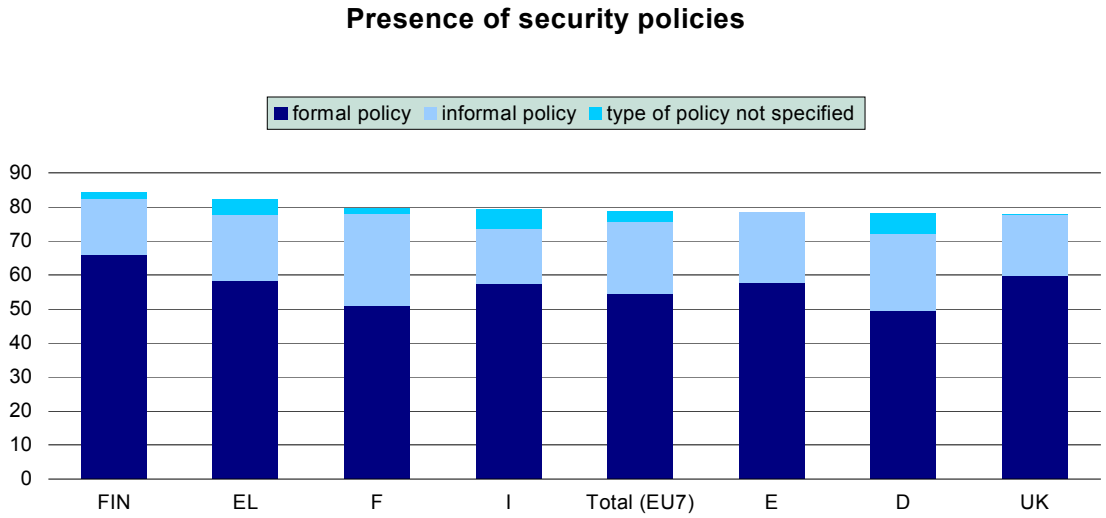


Figure 15 – Presence of security policies in European organisations
Source SIBIS DMS, weighted by employment (N=1857) Businesses with online presence

The chief objective for implementing an information security policy is blocking unauthorised access. As figure 16 shows, this has got high or medium priority for 9 out of 10 enterprises, Europe-wide. In fact, blocking unauthorised access can be seen as the raison d'être of any information security policy. However, European businesses also ascribe very high priority to budget expansions and internal definition of the security architecture. With the notable exception of France, only outsourcing of security management is a lower priority.

36 See Security and Trust, Indicator Handbook, SIBIS WP 6, p. 6

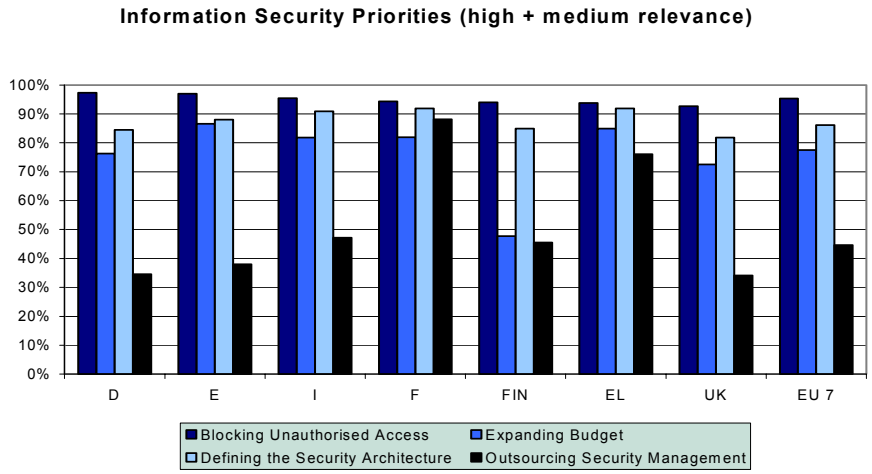


Figure 16 – Information security priorities for European businesses
Source SIBIS DMS, weighted by employment (N= 1857) Businesses with online presence

5.3 Analysis of Compound Indicators

Indicators piloted through the SIBIS survey are a useful means for the development of compound *indicators*, i.e. a combination of different yet related indicators. Such combinations are helpful to scale measures in order to facilitate comparisons otherwise difficult to perform. Through weighted averaging, compound indicators take care of differences in size, units etc. putting the information in a uniform and 'unitless' footing. Hence, a compound indicator can be a practical instrument to compare different EU states with regard to their performance in the Information Society when it comes to security of information infrastructures.

For example, one might think of an index to assess the severity of damages caused by different sorts of breaches suffered by today's European organisations. Decision Makers' indicators, piloted through the DMS, can be the right means to provide this information. In this example, the compound indicator shall be named DSI (Damage Severity Index).

The DSI measures the severity of damages caused by the five sorts of breaches (ID theft, on-line fraud, manipulation of software applications, computer viruses and unauthorised entry to internal networks). It is a weighted average measuring how substantial the damages of these incidents were. Weights have been allocated as follows:

5 = very substantial,
3 = rather substantial and don't know
1 = not substantial

Therefore, values range from 1 (if no damages at all were suffered) to 5 (if damages were always very substantial). As can be expected, no country scores 1 or 5. Greece is the country where breaches caused most damages, while Finland is the country where least damages were suffered.[37] This index is in fact a mean of five distinct indices, each associated to the damages caused by each of the five breaches, and can be expressed by the following formulae:

$$DSI = \frac{\sum_{i=1}^{n} (Subindex)n}{n}$$

With

$$DSI(Subindex) = \frac{\sum_{i=1}^{n} w_{xi} f_{xi}}{\sum_{i=1}^{n} f_{xi}}$$

Where:

[37] Again it must be borne in mind that the extremely limited number of respondents in Greece does not allow us to formulate any convincing conclusion on this country.

w_{xi} = the type of security breach suffered (ID Theft, on-line fraud, manipulation of software application, computer viruses and unauthorised entry in internal networks), weighted

f_{xi}=weighted frequency per answer category

(Weighted by employment)

n = the number of reported types of security breaches suffered per country (in this study 4 or 5)

i = sub-index number

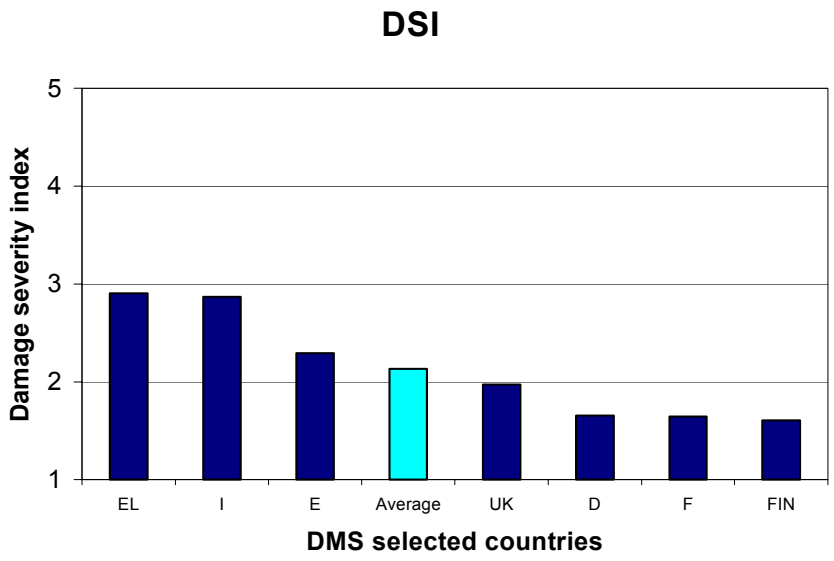


Figure 17 –Damage Severity Index
Source SIBIS DMS, weighted by employment (N=514) Businesses with online presence that suffered security breaches in the last 12 months

6. Conclusions and Further Developments

This study began with the premise that information and network security is a fundamental component for ensuring the widest possible participation in the Information Society. Not just citizens, who might refrain from using possibly unsafe infrastructures, but also businesses and governments, are key players in the game. Though businesses ought to assure consumers' privacy, they also wish to gain from information on customers' purchasing behaviour and characteristics; governments, for their part, balance these different interests, i.e. citizens' right to privacy and security, and businesses' right to obtain customer information in order to maximise their profits. With this in mind, the indicators developed within SIBIS had the aim of filling gaps in current statistical coverage on important issues such as security and trust. These indicators provide a picture on how Europe is performing in its efforts to build a successful, secure and trustworthy Information Society. Two complementary surveys, covering nine topics, were conducted in the SIBIS project. The survey of citizens covered the EU Member States, the USA and Switzerland. The survey of businesses covered Finland, France, Germany, Greece, Italy, Spain and the United Kingdom. The purpose for that part of the survey that dealt with security and trust was to query citizens and businesses on their experience in terms of security incidents, their 'security-awareness' and behaviour, and the conditions for an optimal co-operation in the field. The work presented here, however, is just the first step and will soon be complemented by new results of the GPS survey, recently held in the ten NAS (Newly Associated States).

In the course of the analysis we have implied that Europe is progressing in terms of trust and security. However, the GPS findings also suggested that, to this day, the US is the leading force when it comes to citizens' security-aware and conscious behaviour. For example, while more than 40% of regular US Internet users are aware of security features of websites, such as the deployment of anti-virus protection, this figure is lower than 20% in the European Union. Also, the impact of security concerns on people's willingness to shop or bank on-line is by far stronger in Europe than in the United States, although there are national specifications.

On the whole, GPS data on security and trust depicts a European Union of highly concerned people, who more often than not are prevented from buying on-line because of these concerns, and are often unaware of security features of websites, nor do they keep them in mind once they finally decide to shop over the Internet. In spite of this, citizens seem eager to report violations of their on-line privacy and confidentiality to a third independent party, and are keen to do so openly. Also, findings suggest that Europe is divided between north and south on a number of issues. In central and northern Europe, for instance, e-Commerce is by far more common and the awareness and importance of security features of websites is higher than in the Mediterranean areas. The propensity to report on-line violations, however, is similar across the Union.

The DMS portrays European businesses as generally protected against most breaches by a (formal) information security policy, but nevertheless extremely vulnerable to computer virus infections, believed to originate in most cases from external hackers or internal users rather than from competitors or customers. Although it is generally believed that businesses are more concerned about the impact of hacking or dedicated

high scale network intrusion than viruses, deemed a greater threat to home computing and consumers, SIBIS shows that against viruses, European organisations have their toll to pay: from north to south 41% of businesses, on average, suffered 'very' or 'rather' substantial consequences of computer virus infections. Moreover, being informed on the occurrence of breaches is still an internal affair for most organisations: outsourced security services are an exception and managers generally rely on their own information security systems. However, on certain issues also European businesses suffer from a longitudinal split. For example, while the incidence of viruses is significant across all surveyed countries, their consequences appear worse in southern than in northern Europe. In the former, up to 60% of the respondents admitted suffering substantial damages, in the latter this percentage drops to less than 40%.

It is clear then that, notwithstanding European progress and efforts, much still needs to be done in order to redress these problems and divides. Not always the way is straightforward nor the means to achieve a truly inclusive information society, evident. For example, this research clearly showed that the option of reporting on-line violations anonymously would hardly turn into an appreciable increase in people's propensity to report. Different kinds of incentives seem necessary to encourage people to report on-line violations. Similarly, though computer viruses are the only significant security breach today's organisations have to face, it is crucial to limit the consequences and, at the least, to level them out among different member states; as long as southern Europe is perceived as visibly more unsafe than northern Europe, investments there risk stagnation.

Although the issues covered in this report are relevant to an improved understanding of the progress and change in the domain of trust and security of information systems, there are more: more have been identified, but within the limitations of the SIBIS project it was not possible to explore them all in depth. Notwithstanding the results of these research activities, project time and financial restrictions have prevented from examining other important elements of public and commercial concerns about information and network security. First, more needs to be directed towards understanding on identifying specific priorities for the definition of information and network information security policies inside public and private organisations. A second area needing more research refers to appreciating how to quantify the returns on investments in information and network security technologies and processes. In this context, a possibility would be to undertake some stated preference survey exercises to try to assess how information and network technologies induce users to change their online behaviours. Finally, more work is needed in trying to correlate SIBIS data with cyber crime statistics. However, this last point requires that both public and private organisations develop a framework through which they can exchange information and network security related data and statistics.

7. References

Bob Cohen, 'New Poll Finds Americans Concerned About Security of Government Computers', Infosec Outlook, vol. 1 n.7, September 2000

Broadbent, M. and Lofgren H., 'Information Delivery: Identifying Priorities, Performance and Value', Information Processing and Management, vol. 29 n. 6, 1993

Cheskin Research and Studio Archetype/Sapient, E-Commerce Trust Study, January 1999

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

Consumers' International, Shop On-line 2001: An International Comparative Study of Electronic Commerce, September 2001

Corrocher, N., "Internet Diffusion in Europe: demand scenarios and the digital divide", Issue Report n.29, Università Bocconi, Databank Consulting, July 2002, STAR project, http://www.databank.it/star

CSI/FBI, Computer Crime and Security Survey, S. Francisco, April 2002

Donna Hoffman, Thomas Novak and Marcos Peralta, 'Building Consumer Trust On-line', Communications of the ACM, vol. 42 no.2, April 1999

eEurope 2002, An Information Society for All, Action Plan prepared by the council for the Feira European Council, 19-20 June 2000, Brussels, 14 June 2000

Electronic Privacy Information Center (EPIC) and Ruchika Agrawal, Non-Commercial Constituency Representative on the WHOIS Task Force Before the GNSO Council, *PRIVACY ISSUES REPORT: The Creation of A New Task Force is Necessary For an Adequate Resolution of the Privacy Issues Associated With WHOIS*, March 2003

GVU's Tenth WWW user Survey, October 1998

Human Firewall Project, available at http://www.humanfirewall.org

IT Analysis, 'Internet attacks on the rise', The Register, 10 July 2002

John Butler, 'Towards Understanding and Measuring Conditions of Trust: An Inventory', The Journal of Management, vol.17 no.4, April 1991

Lorenzo Valeri, Dot.com versus Dot.gov: States, Businesses and an International Regime for Information Assurance, PhD Dissertation completed at the Department of War Studies, King's College London, 2001

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

National Research Council, Trust in Cyberspace, Washington, DC, USA: National Academy Press, 1999

Robert Morgan and Shelby Hunt, 'The Commitment-Trust Theory of Relationship Marketing', The Journal of Marketing, vol. 58 no.3, July-September 1994

Stephanie Daman, Andrew Rathmell, Lorenzo Valeri, Information Risk: Implications for the Financial Sector, Study undertaken under contract to: Foresight Directorate Office of Science & Technology, Department of Trade & Industry –United Kingdom, Final report, 10 May 2002

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.

Taylor, A, and Farrell, F., Information Management for Business, London: ASLIB Press, 1994

8. Abbreviations

CIP	Critical Infrastructures Protection
DMS	Decision Makers Survey
GPS	General Population Survey
DK	Don't Know
DSI	Damage Severity Index
IS	Information Society
PA	Public Administration
PKI	Public Key Infrastructure

9. Annex – Methodology of the survey

9.1 General Population Survey (GPS)

Outline of the study

The survey was conducted in April-May 2002 in all 15 EU Member States plus Switzerland and the USA, using computer-aided telephone interviews. The survey was co-ordinated and executed by INRA, Germany. The population for this study is all persons aged 15 and over living in private households in the respective countries and speaking the respective national language(s). In Switzerland the survey was carried out in the German and French speaking parts of the country; in the USA the population includes English speaking people in the 48 continental federal states of the USA (excluding Alaska and Hawaii); in Finland, Finnish speaking population was interviewed. Subject discussed included ownership and use of ICT equipment, use of the Internet and e-commerce activities, competence in the use of new media, questions on health and the Internet, the Internet and security concerns, e-government, telework, mobile work and other new ways of working, as well as further education and satisfaction with working conditions. 11,832 interviews were successfully completed. The average interview length per country varied between 10 and 20 minutes.

Field Report and Outcomes

		B	DK	D	FIN	F	EL	UK	IRL	I	L	NL	AT	P	S	CH	E	USA
Method		C.A.T.I.																
1	gross sample (utilised addresses)	4506	3154	9999	2621	7300	5022	11392	3890	12006	8764	3640	4669	1403	5177	2327	6494	18162
1.1.	non-contacts – thereof:	311	242	1701	40	3401	2346	139	1111	4436	5023	803	193	91	455	638	1239	4192
1.1.1	unobtainable	0	235	1202	0	2342	2077	123	654	4436	3748	522	124	43	113	638	644	3656
1.1.2	engaged	3	7	436	0	57	206	1	316	0	705	164	8	32	55	0	5	536
1.1.3	answer phone, fax, modem	308	0	63	40	1002	63	15	141	0	570	117	61	16	287	0	590	0
1.1.4	other	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.2	sample neutral non-response – thereof:	1874	1917	4492	984	511	1022	5088	1051	2659	1316	805	2322	410	2808	322	1095	8789
1.2.1	invalid telephone numbers	955	1516	3760	97	60	529	4308	498	1657	790	652	858	334	2297	230	398	5725
1.2.2	not in the population	472	202	41	782	374	176	119	405	364	0	153	1248	47	16	0	164	478
1.2.3	business numbers	300	82	285	12	27	220	437	0	340	455	0	75	15	193	0	434	1331
1.2.4	other	147	117	406	93	50	97	224	148	298	71	0	141	14	302	92	99	1255
2	net sample – thereof:	2321	995	3806	1597	3388	1654	6165	1728	4911	2425	2032	2154	902	1914	1367	4160	5181
2.1	refusal	1470	468	2451	912	2231	747	5012	1134	3592	1000	1248	1609	364	1246	529	2255	3198
2.2	termination	114	0	87	0	30	0	80	11	201	0	0	1	6	19	0	115	143
2.3	target person contacted but interview impossible – thereof:	152	26	267	16	127	402	73	83	118	925	254	44	32	146	316	775	836
2.3.1	possible appointment outside field time	0	23	14	1	23	9	26	14	106	763	208	7	6	30	80	321	156
2.3.2	appointments to continue interview outside field time	152	0	200	0	104	295	47	65	12	17	11	34	18	24	194	179	669
2.3.3	other	0	3	53	15	0	98	0	4	0	145	35	3	8	92	42	275	11
2.4	complete interviews	585	501	1001	669	1000	505	1000	500	1000	500	530	500	500	503	522	1015	1004
3	exhaustion rate (%) (2.4/(2.1+2.2+2.4))	27.0%	51.7%	28.3%	42.3%	30.7%	40.3%	16.4%	30.4%	20.9%	33.3%	29.8%	23.7%	57.5%	28.5%	49.7%	30.0%	23.1%

Weighting

1. Transformation from household sample to person sample

As only one person per household is interviewed, the described sample procedure provides a household sample, i.e. each household of the base population has the same likelihood of being in the sample but not each person. With the weighting stage of the transformation the equal likelihood of households is replaced mathematically by the equal likelihood of the individuals. To this end, each data set is multiplied by the amount of people in the household aged 15 or over. This number is subsequently divided by the average household size in order to obtain the actual case number.

2. Adjustment of the unweighted sample structure to the official statistic

Because random samples are not evenly distributed across all population strata, the distribution of unweighted samples regularly and systematically deviate from the population distribution from official statistics. Through the mathematical weighting the sample distribution is adjusted to the official statistics. The national weighting factor (P10), which results from the iterative weighting, was included in the data material. To this end the following criteria are used in the respective countries.
Austria: age, gender, region; **Belgium**: age, gender, region, locality size; **Denmark**: age, gender, region; **Germany**: age, gender, region, locality size; **Greece**: age, gender, locality size; **Finland**: age, gender, region; **France**: age, gender, region, locality size; **Ireland**: age, gender, region; **Italy**: age, gender, region, locality size; **Luxembourg**: age, gender, region, locality size; **Netherlands**: age, gender, region; **Portugal**: age, gender, region, locality size; **Sweden**: age, gender, region; **Switzerland**: age, gender, region; **Spain**: age, gender, region, locality size; **UK**: age, gender, region; **USA**: age, gender, region, locality size.

3. Adjustment of the weighted sample structure to the EU 15- member states population

This weighting factor was necessary to calculate total figures according to the whole population of the European Union member states. Furthermore it is useful to compare the EU with the US. Population sizes of each member state are weighted to reduce the distortion based on the sample sizes in each country. The different country-specific weighting factors are the following:

Austria	0.44	Italy	1.63
Belgium	0.48	Luxembourg	0.02
Denmark	0.29	Netherlands	0.80
Germany	2.29	Portugal	0.55
Greece	0.59	Spain	1.09
Finland	0.21	Sweden	0.48
France	1.56	United Kingdom	1.57
Ireland	0.20	*Switzerland, USA*	*none*

9.2 Decision Makers Survey (DMS)

Outline of the study

The survey was conducted in March-May 2002 in seven EU Member States using computer-aided telephone interviews. The survey was co-ordinated and executed by INRA, Germany. The population for this study is defined as all establishments belonging to four aggregated industry sectors in the seven Member States. The interview was conducted with IT responsible persons in companies across all sectors of the economy. Subjects discussed included ownership and use of ICT equipment, use of the Internet and e-commerce and e-business activities, e-business security, e-government, web-site accessibility and ICT in research and development. 3,139 interviews were successfully completed. The average interview length per country varied between 14 and 18 minutes.

Methodology

Field Report outcomes

		D	FIN	F	EL	UK	I	E
1	Sample (gross), i.e. number dialled at least once	4917	1923	8061	1728	8726	10846	8489
1.1	Telephone number does not exist	787	47	598	43	416	1160	808
1.2	Not an establishment (i.e. private household, etc.)	46	15	0	2	0	0	235
1.3	Fax machine/ Modem	81	0	152	31	0	0	519
1.4	Quota completed, therefore address not used	0	849	1599	2	2659	848	1397
1.5	No target person in establishment	858	226	1261	35	1766	822	2043
1.6	Language problems	0	15	0	0	0	0	10
1.7	SUM (1.1+1.2+1.3+1.4+1.5+1.6)	1753	1152	3610	113	4841	2830	5012
2	Net sample (1 minus 1.7)	3164	771	4451	1615	3885	8016	3477
2.1	Nobody picks up phone (and max. contacts not yet exhausted)	325	2	326	229	32	804	18
2.2	Line busy, engaged	45	0	31	235	2	1852	9
2.3	Answering machine	111	4	82	15	0	0	482
2.4	Contact person refuses (i.e. refusal at reception, switchboard)	436	228	912	38	1354	1056	1022
2.5	Target person refuses	1044	204	1569	107	1672	1410	896
2.6	no appointment during fieldwork period possible	33	14	356	36	176	680	203
2.7	open appointment	604	4	642	644	52	1668	111
2.8	target person is ill/ cannot follow the interview	1	3	18	0	0	0	18
2.9	Interview abandoned	53	1	14	4	97	34	102
2.10	Interview error, cannot be used	0	5	0	6	0	0	109
2.11	SUM (2.1+2.2+2.3+2.4+2.5+2.6+2.7+2.8+2.9+2.10)	2652	465	3950	1314	3385	7504	2970
2.12	SUCCESSFUL INTERVIEWS	512	306	501	301	500	512	507
3	Completion Rate (2.12 / (2.11+2.12)), in %	16.18	39.69	11.25	18.63	12.87	6.38	14.58

Target and actual number of interviews

			F	D	I	E	UK		FIN	EL
Quota Group		required	- achieved -					required	- achieved -	
I Manufacturing, construction, primary sector	1 - 9	*30*	33	30	34	33	32	*18*	18	17
	10 - 49	*35*	36	36	37	35	35	*21*	21	22
	50 - 199	*35*	38	37	40	35	35	*21*	21	25
	200 - 499	*40*	44	41	43	41	40	*24*	28	22
	500+	*15*	9	14	13	15	15	*9*	9	6
	Sum	155	160	158	167	159	157	93	97	92
II Distribution, catering, transport and communication	1 - 9	*45*	50	47	45	46	45	*27*	28	27
	10 - 49	*40*	42	41	41	43	40	*24*	24	25
	50 - 199	*30*	28	31	26	30	30	*18*	18	18
	200 - 499	*15*	19	15	16	15	15	*9*	5	9
	500+	*10*	5	10	8	10	10	*6*	5	6
	Sum	140	144	144	136	144	140	84	80	85
III Financial and business services	1 - 9	*30*	32	30	34	30	30	*18*	16	17
	10 - 49	*20*	19	21	23	21	20	*12*	14	11
	50 - 199	*10*	13	10	17	10	10	*6*	6	8
	200 - 499	*10*	13	10	6	10	10	*6*	7	6
	500+	*10*	8	9	4	7	8	*6*	6	6
	Sum	80	85	80	84	78	78	48	49	48
IV Public administration, education, health, other personal and social services	1 - 9	*20*	20	24	19	20	20	*12*	13	13
	10 - 49	*25*	29	25	26	25	25	*15*	16	16
	50 - 199	*30*	22	30	34	30	30	*18*	18	18
	200 - 499	*35*	32	35	31	35	35	*21*	23	20
	500+	*15*	9	16	15	16	15	*9*	10	9
	Sum	125	112	130	125	126	125	75	80	76
	Total	*500*	501	512	512	507	500	*300*	306	301

Weighting

For the SIBIS DMS a sample stratified by sector/ size cells was used which ensured that in each sector, establishments from all size classes were sampled. In order to be able to raise figures to national level, some form of weighting is required which adequately reflects the structure and distribution of establishments (or related variables) in the universe of the respective country (and, by implication, EU15). All presentation of SIBIS results indicates clearly which of these weighting schemes was used.

Original Weighting

Within each country, the interviews were split according to a quota plan which guaranteed that the sample is not dominated by micro and small companies. The quotas roughly reflect the distribution of employment over sector and establishment size bands in the EU, and derive from research into establishment sampling frames undertaken for previous studies by Infratest and GfK in the course of ECaTT. They represent best estimates, but do not take account of country differences.

The quota scheme looks as follows:

empirica			SUGGESTED QUOTAS: Sectors (aggregated) X Size											
			1- 9		10 - 49		50 - 199		200 - 499		500+		Total	
			% of total	abs	% of total		% of total		% of total		% of total		% of total	
Quota I	Manufacturing, Construction, Primary Sector, includes:		6%	30	7%	35	7%	35	8%	40	3%	15	31%	155
	1	Mining, Energy												
	2	Manufacturing												
	3	Construction												
Quota II	Distribution, Catering, Transport & Communication includes:		9%	45	8%	40	6%	30	3%	15	2%	10	28%	140
	4	Distribution												
	5	Hotels, Restaurants												
	6	Transport, Communication												
Quota III	Financial & Business Services includes:		6%	30	4%	20	2%	10	2%	10	2%	10	16%	80
	7	Banking, Insurance												
	8	Business Services												
Quota IV	Public administration, education, health, other personal & social services includes:		4%	20	5%	25	6%	30	7%	35	3%	15	25%	125
	9	Public Administration												
	10	Education												
	11	Health and Social Work												
	12	Other personal or social services												
		Total	25%	125	24%	120	21%	105	20%	100	10%	50	100%	500

(The absolute numbers refer to countries with n=500)

Weighting was used in cases where the quotas could not be reached exactly in line with this quota plan (mostly due to the limited absolute number of establishments in the two biggest size classes). Note that because of the use of a single quota plan for all countries, country differences in the distribution of employment over establishment size bands which occur in reality are not reflected in the data. This is due the lack of available data on the distribution of employment across establishments size bands in almost all EU Member States, and constitutes a considerable problem. This weight is therefore not used for presenting SIBIS results.

Weighting by employment

The data available on the distribution of employment over establishment size bands is very limited for most EU Member States. SIBIS used data from a variety of sources, including:

- BT database (United Kingdom)
- ISTAT Industry and Services Intermediate Census – latest available, 1996 (Italy)
- National Statistical Service of Greece - latest available, 1995 (Greece)
- SIREN (France)
- Tilstokeskus Official Statistics (Finland)
- Heins + Partner B-Pool (Germany)
- Schober Business Pool (Spain)

and adjusted using data from the DG Enterprise/ Eurostat SME Database (latest available, 1997), to estimate the establishment/ employment structure for each country in the sample. The table below shows the resulting establishment size structure per country.

		Country							
		D	E	EL	F	FIN	I	UK	*EU7*
Establishment size band	1 to 9	23%	23%	59%	17%	13%	38%	14%	*23%*
	10 - 49	19%	28%	16%	22%	16%	22%	31%	*24%*
	50 - 199	21%	21%	8%	21%	19%	14%	26%	*20%*
	200 - 499	13%	9%	6%	14%	16%	7%	13%	*12%*

	500 and more	25%	18%	10%	25%	37%	19%	17%	*21%*
Total	Column %	100%	100%	100%	100%	100%	100%	100%	*100%*

Using this weight, the weighted sample for each country therefore reflects employee distribution between the five establishment size bands within that country. This means that a data reference of, for example, ”20% of all establishments in country A” should be understood to mean ”establishments accounting for 20% of all employees in country A”.

Weighting by employment for EU-7 average

Additionally another weighting factor was created to calculate average figures for all countries in the sample (which together represent roughly 82% percentage of total EU employment). Each country is represented in this weight according to its share in the total employment of the 7 EU countries in which the survey was conducted.

9.3 Questionnaires

9.3.1 Questionnaire for the General Population Survey (GPS)

Structure of the questionnaire:

Module IN: Introduction and screening
Age
Educational attainment
Employment status
Occupation
Type of organisation
Main working place

Module A: Basic ICT equipment access and use
Use of computer
Use of e-mail
Internet access and use
Methods of Internet access
Effects of Internet use
Barriers to using the Internet
Access to mobile phone
Mobile data services
Effects of mobile phone use

Module B: E-commerce and other uses of the Internet
Online activities
Barriers to buying online

Module D: Skills
Internet user experience and know-how

Module L: e-Health
Use of online health information
Perception regarding the trust placed in online health information provider

Rationale for health info search

Module J: Security
Security concerns
Reporting of security violations
Security-related awareness and behaviour

Module K: e-Government
Preference for e-Government services
e-Government experience
Barriers to e-Government

Module E: Telework
Home-based telework
Intensity of home-based teleworking
Duration of telework:
Financing of tele-workplace
Interest in telework:
Perceived feasibility
Effects of telework

Module F: Mobile work
Mobile work (Intensity):
Mobile telework

Module G: Tele-cooperation/Tele-collaboration
Co-operation with external contacts using ICTs
e-Lancing

Module H: Outcomes of work
Work-family balance
Job quality
Job satisfaction

Module C: Educational attainment and lifelong learning
Company-provided training
Training provided by other organisations
Self-directed learning
Modes of training (use of eLearning)

Module Z: Standard demography
Household size
Disability
Income

Module J: Security		**GPS**
Transition J *IF A7=1*	Now the topic is internet security.	
J1 *IF A7=1*	How concerned are you about .[item]: Are you ... *[INTERVIEWER: Read out answer categories]* (a) data security on the Internet, i.e. the loss or manipulation of your data? (b) privacy and confidentiality on the Internet, i.e. personal information about you being misused by third parties?	FOR EACH (1) very concerned (2) somewhat concerned (3) not concerned (4) DK
J2 *IF J1(a)=1,2 or J1(b)=1,2*	Are these concerns stopping you from using the Internet to buy goods or services online: often, sometimes, or never?	(1) often (2) sometimes (3) never (4) DK
J3 *IF A7=1*	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? *[INTERVIEWER: Read out answer categories]*	(1) yes, very likely (2) maybe (3) no (4) DK
J4 *IF J3=1,2,3*	Would it be easier for you to do so if you could do it anonymously?	(1) yes (2) no (3) DK
J5 *IF A7=1 & (B1(b)=1 or B1(c)=1)*	How often are you aware of security features of websites when you use the Internet to buy online: often, sometimes or never?	(1) often (2) sometimes (3) never (4) DK
J6 *IF A7=1 & (B1(b)=1 or B1(c)=1)*	And how often do you take security features of websites into account when deciding about whether to buy online: often, sometimes or never?	(1) often (2) sometimes (3) never (4) DK

9.3.2 Questionnaire for the Decision Maker Survey (DMS)

Structure of the questionnaire:

Introduction and Screener Section

Module A: Basic characteristics
Type of organisation
Number of staff (employees)
Turnover

Module B: Module B: Basic ICTs take-up and intensity of use (e-Business)
e-Mail
Internet
Intranet
EDI
Video-conferencing
Call-centre
Staff access to ICTs

Module C: e-Commerce
Website/ Internet presence
Online sales
Barriers to e-commerce (selling)
Benefits from / Outcomes of e-commerce
Online procurement
Barriers to online procurement
Benefits from/ Outcomes of online procurement
Online supply chain integration
e-Marketplaces

Module D: e-Business security
Security breaches
Information security strategy
Barriers to security
Security provisions

Module F: e-Government
Use of e-Government services
Barriers to e-Government

Module G: Website accessibility
Design for all" / "universal design" principle awareness

Module E: R&D
R&D staff
Computer staff in R&D unit(s)
IT staff providing computer services to R&D
Outsourced computer services for R&D
Vacancies in IT for R&D

Module D: e-Business security		**DMS**
Transition D *IF C1=1*	Let us now turn to the topic of information security. Again, please refer to your establishment when answering.	
D1 *IF C1=1*	Many establishments are affected by security breaches such as identity theft, online fraud, manipulation of software applications, computer viruses or unauthorised entry to internal networks. Have any breaches of your information security occurred in your establishment in the last 12 months?	(1) yes (2) no (3) DK
D2a *IF D1=1*	***Progr.: Note for D2a to D2b:*** ***For each item in D2a=1, ask directly D2b; then go to next item in D2a!!*** Which of the following types of information security breaches have occurred in your establishment in the last 12 months? Did you experience cases of ... [item]? INT.: READ OUT. ONE ANSWER PER ITEM. (a) Identity theft (b) Online fraud (c) Manipulation of software applications (d) Computer virus infections (e) Unauthorised entry to internal networks	FOR EACH: (1) yes (2) no (3) DK
D2b *(For Each Item) IF D2a=1*	And how substantial were the consequences of this security breach for your establishment? Would you say they were ... INT.: READ OUT ANSWER CATEGORIES. SINGLE ANSWER (PER ITEM ASKED)	FOR EACH ITEM IF D2a=1 (1) very substantial (2) rather substantial (3) not substantial (4) DK
D3 *IF D1=1*	Where do you believe these breaches mainly came from? Do you think the largest threat to online security came from ... INT.: READ OUT ANSWER CATEGORIES. CODE ALL THAT APPLY	MULTIPLE ANSWERS (1) Customers (2) Suppliers/competitors (3) Former employees (4) Computer hackers (5) Internal users (6) Others, not mentioned yet (7) DK
D4 *IF D1=1*	How have you learned about these breaches, in most cases? Were you ... [item] INT.: READ OUT, CODE ALL THAT APPLY	MULTIPLE ANSWERS (1) alerted by a customer/supplier (2) alerted by employees or did you notice yourself (3) notified by your own information security system (4) made aware by damage or loss of data (5) alerted by the providers of outsourced security services (6) in another way (DO NOT READ) (7) DK
D5 *IF C1=1*	Does your establishment or your organisation have an information security policy?	(1) yes (2) no (3) DK
D6 *IF D5=1*	How would you describe it? As formal or informal?	(1) formal (2) informal (3) DK

D7 *IF D5=1*	Which are your information security priorities? How much priority is given to ... [item] INT.: READ OUT ANSWER CATEGORIES. ONE ANSWER PER ITEM. (a) Blocking of unauthorised access (b) Expanding budget for security measures (c) Defining the security architecture (d) Outsourcing security management	FOR EACH (1) high priority (2) medium priority (3) low priority (4) DK
D8 *IF C1=1*	How important are the following factors as barriers to effective information security inside your establishment? How about ...[item]: Is this factor as a barrier to effective information security inside your establishment... INT.: READ OUT ANSWER CATEGORIES. ONE ANSWER PER ITEM. (a) High costs for security measures (b) Lack of staff training (c) Lack of staff time (d) Complexity of the technology (e) Lack of employee co-operation	FOR EACH: (1) very important (2) fairly important (3) not important (4) DK
D9 *IF C1=1*	Which of the following tools do you use for information security in your establishment? Do you make use of ... [item] INT.: ONE ANSWER PER ITEM. (a) Control of access to the computer system (b) Cryptography/ data encryption (c) Vulnerability Assessment Tools (d) Firewalls (e) Security Training and Awareness Rising Activities (f) Intrusion Detection Systems (g) End-user Security Training Classes	FOR EACH: (1) yes (2) no (3) DK