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.

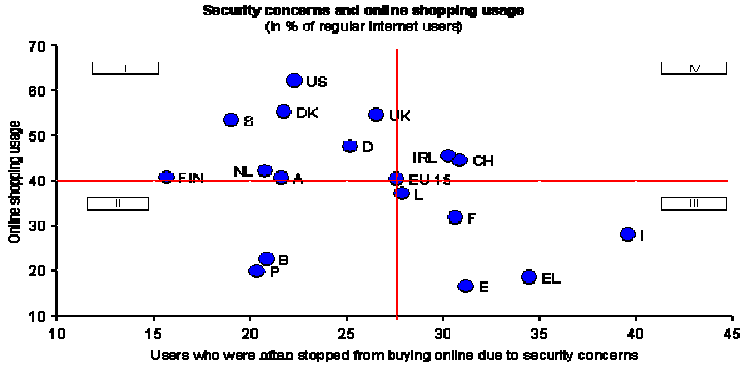

Figure 1 – Security Concerns and on-line Shopping Usage

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].

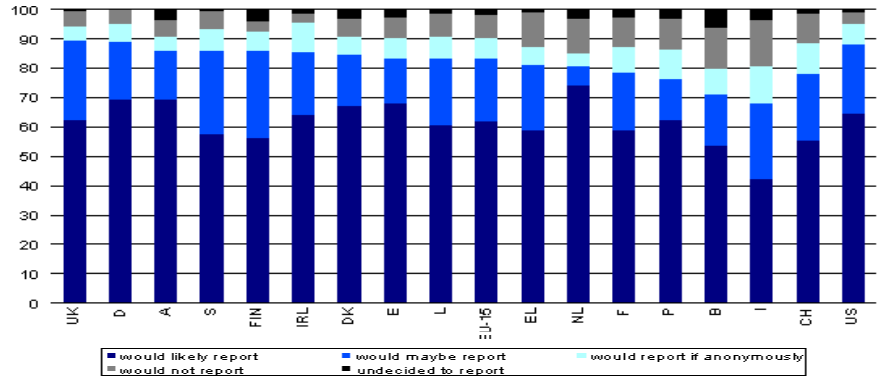

Figure 2 – Reporting of on-line Violations

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.

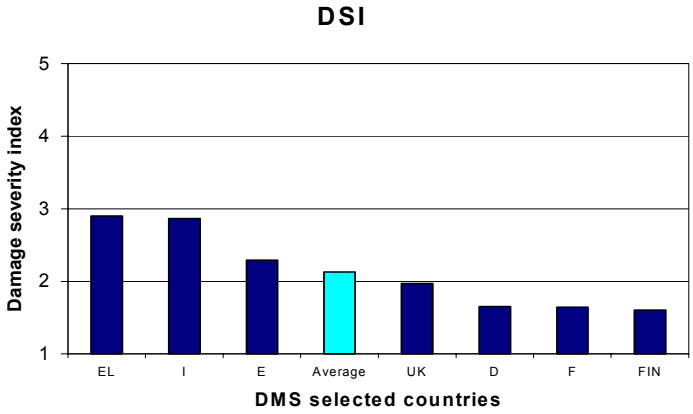

Figure 3 – Damage Severity Index

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.

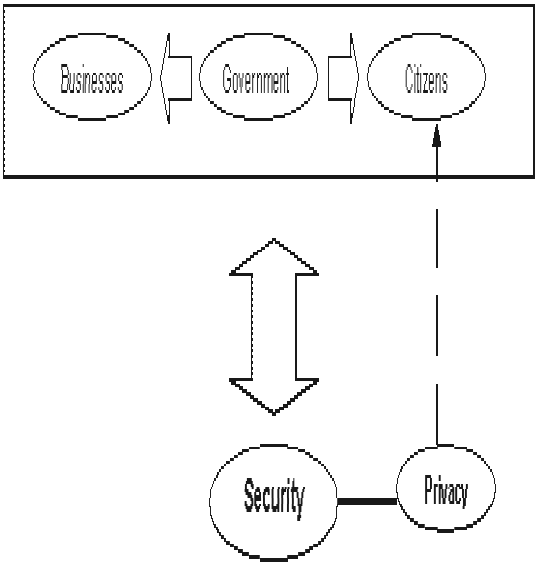

Figure 4 – Stakeholders and their Interactions

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.