3 Security and trust

3.1 Domain Description

Concerns about security of electronic networks and information security have been growing along with the rapid increase in the number of network users and the value of their transactions. The perception of insufficient protection by citizens and businesses is a potential impediment to the development of the information society. In fact, one of the enabling elements to create an information society in Europe is a fast and secure Internet. However, “secure” should not only be seen in terms of secure technology, but wider than that: both technical security measures and security as perceived by consumers and organisations (“trust”) are important. Current policy literature and statistical indicators provide the basis for identifying the gaps and the kind of information needed to fill them. The process of identifying gaps together with exploring existing indicators allows the development of a vision on what new indicators could complement current policy needs for information.

In order to do this, it is important to look at both, the supranational and the national level. In fact, while, collaboration on the issue of trust and security at a supranational level is a rather recent phenomenon (with some experience on the law enforcement side such as information exchange and collaboration between police forces), the national level has a longer history and deeper insights on these topics.

An adequate set of reliable indicators is necessary in order to know where eEurope stands today and what direction it needs to take for the future. An analysis of the policy literature and of indicators being used today highlights the main relevant issues at stake concerning security and trust, such as:

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

Based on these issues the major problems in statistical coverage as well as viable solution can be identified. A set of new indicators is proposed to help redress the current lack in cross-country statistics in this area.

3.2 Description of major problems and gaps in statistical coverage

SIBIS defines **security** as *the combination of technical and managerial processes that aim to foster confidentiality, privacy, integrity & availability of data and information systems, as well as to provide authentication and non-repudiation functionalities*. As concerns "trust", a fundamental problem is that trust is not a single *representative*, *useful* and *agreed* objective to

be used for benchmarking. The review of the various possible definitions of “trust” offered by literature on the topic confirms the need to reject the use of a single indicator measuring trust and concentrate, instead, on the measurement of three distinct indicators for security. At the same time the analysis suggests the identification of *units of analysis* (governments, businesses and individuals) which should guide data collection based on surveys and existing indicators.

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

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

3.3 New indicators overview

In order to address the highlighted difficulties, three thematic domains are suggested for benchmarking online security:

- On-line malicious activities
- Prevention of malicious activities and downtime
- On-line interaction facilitators

Specific indicators, referring to the three Security benchmark indicators may be split between level-1 and level-2 indicators. While all indicators selected for inclusion in the SIBIS survey are “level 1”, nonetheless, some relevant indicators could not be included because of budgetary constraints. The following tables list the “level 1” indicators, specifying whether or not they are included in the survey.

Thematic Domain	Selected new level 1 indicators	Piloting in SIBIS
On-line malicious activities	Ÿ Security breaches occurred in the organisation	SIBIS DMS
	Ÿ Type and relevance of breaches suffered	SIBIS DMS
	Ÿ Supposed origin of breaches	SIBIS DMS
Prevention of on-line malicious activities and downtime	Ÿ Concern regarding on-line security	SIBIS GPS
	Ÿ Source of information on occurred breaches	SIBIS DMS
	Ÿ Presence of security policies	SIBIS DMS
	Ÿ Sort of information security policy	SIBIS DMS
	Ÿ Information security priorities	SIBIS DMS
	Ÿ Barriers to information security	SIBIS DMS
	Ÿ Tools of information security	SIBIS DMS
	Ÿ Importance attributed to information security	—
	Ÿ Comprehension of Private Sector's Security Requirements by the Public Sector	—
	Ÿ Co-operation of private sector in fostering information security	—
On-line interaction facilitators	Ÿ Perceived security features of websites	SIBIS GPS
	Ÿ Effects of Security concerns on on-line shopping behaviour	SIBIS GPS
	Ÿ Propensity to report incidents of on-line violations without assurance of anonymity	SIBIS GPS
	Ÿ Propensity to report incidents of on-line violations under assurance of anonymity	SIBIS GPS
	Ÿ Effects of perceived security features of websites on consumers' propensity to shop on-line	SIBIS GPS
	Ÿ Quality assurance and commitment of on-line merchants to security	—
	Ÿ Companies' information about on-line security	—

Particular attention is given to identifying possible approaches for combining traditional and innovative indicators in order to derive a single aggregate measure. However, since they represent different domains, the three thematic domains should be kept separate. In fact they cannot be homogenised or compared unless they are quantified using a common base. The multidimensional nature of "trust" prevents us from devising a single benchmarking indicator, and makes us concentrate on the three main thematic domains above. Nonetheless, their overall usefulness is not impinged by this separation. As long as they are interpreted and examined in parallel, the statistical indicators for the three proposed thematic domains can provide policy makers with a useful tool to devise appropriate policies aimed at fostering security for the information society.