OECD publishing

Please cite this paper as:

OECD (2012-12-20), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", *OECD Digital Economy Papers*, No. 214, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5k4dq3rkb19n-en

OECD Digital Economy Papers No. 214

Improving the Evidence Base for Information Security and Privacy Policies

UNDERSTANDING THE OPPORTUNITIES AND CHALLENGES RELATED TO MEASURING INFORMATION SECURITY, PRIVACY AND THE PROTECTION OF CHILDREN ONLINE

OECD

OECD

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

20-Dec-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2011)10/FINAL
Unclassified

Working Party on Information Security and Privacy

IMPROVING THE EVIDENCE BASE FOR INFORMATION SECURITY AND PRIVACY POLICIES

Understanding the opportunities and challenges related to measuring information security, privacy and the protection of children online.

08/05/2012

Christian Reimsbach-Kounatze: christian.reimsbach-kounatze@oecd.org; Tel: +33 1 45 24 76 16

JT03332902

Complete document available on OLIS in its original format

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

English - Or. English

FOREWORD

This report makes a case for improving the evidence base for policy making in areas covered by the Working Party on Information Security and Privacy (WPISP). It provides an overview of existing data and statistics highlighting the opportunities and challenges related to measuring security, privacy and the protection of children online. The report will thus serve as a basis for further discussions with experts in the field to produce guidance for the development of cross-country comparable indicators in the long term.

The report was prepared for the WPISP by Christian Reimsbach-Kounatze (OECD Secretariat). In May 2012, the WPISP agreed to transmit this report to the Committee for Information, Computer and Communications Policy (ICCP) for declassification. The ICCP Committee agreed to its declassification in October 2012.

The report is published under the responsibility of the Secretary-General of the OECD.

---

1. Footnote by Turkey

The information in this document with reference to « Cyprus » relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Turkey recognizes the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Turkey shall preserve its position concerning the "Cyprus issue".

2. Footnote by all the European Union Member States of the OECD and the European Commission

The Republic of Cyprus is recognised by all members of the United Nations with the exception of Turkey. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

© OECD 2012

TABLE OF CONTENTS

FOREWORD 2
TABLE OF CONTENTS 3
SUMMARY 6
INTRODUCTION 8
Building the evidence base 9
Empirical data, statistics, and indicators 9
Surveys 10
Activity reports and related data 10
Internet-based statistics 11
Benefits and limitations in measurement 11
Objectives and methodology 13
Structure 15
INFORMATION SECURITY 16
Official statistics agencies 16
OECD model survey of ICT use by businesses 16
OECD model survey of ICT use by households/individuals 21
Other government and public agencies 25
National and government computer emergency response teams 25
Law enforcement agencies 35
Consumer protection agencies 35
Private organisations and data sources 36
Security tool providers 37
Honey net operators 41
Network services and equipment providers 41
Vulnerability databases 41
Certificate authorities 45
IT consulting, audit and related companies 45
PRIVACY 49
Official statistics agencies 49
OECD model survey of ICT use by businesses 49
OECD model survey of ICT use by households/individuals 49
Other government and public agencies 52
Privacy protection authorities 52
Consumer protection agencies 61
Private organisations and data sources 62
International Association of Privacy Professionals 62
Data breach databases 63
Anonymity surfing and tracking tools 65

PROTECTION OF CHILDREN ONLINE 67
Official statistics agencies 68
OECD model survey of ICT use by households/individuals 68
Other government and public agencies 70
Privacy protection authorities 70
Consumer protection agencies 71
Non-governmental organisations and data sources 71
Parental control and web filtering software vendors 71
Children friendly web content 71
UNDERSTANDING THE POLICY MAKERS' NEEDS 72
Steps of the evidence-based policy making process 72
1. Identifying and defining the problem and its sources 72
2. Measuring the risk and the severity of the potential harm 73
3. Determining whether the risks warrant policy response 73
4. Setting policy objectives and identify the range of policy actions 73
5. Evaluating and selecting policy options 74
6. Developing a review process to evaluate the effectiveness of the policy 74
Identifying the gaps for the policy making process 74
Information security 74
Privacy 75
Protection of children online 75
CONCLUSION 77
NOTES 78
REFERENCES 83
ANNEX 88

Boxes

Box 1. Linking security and privacy data with existing OECD databases 12
Box 2. Security indicators based on surveys of ICT use by businesses 17
Box 3. Security indicators based on surveys of ICT use by households/individuals 22
Box 4. The role of Computer Emergency Response Teams (CERTs) 26
Box 5. Security indicators based on CERT data 32
Box 6. Indicators on online fraud in the Consumer Sentinel Database 36
Box 7. Some anecdotal evidence related to security 37
Box 8. Malware statistics 38
Box 9. Measuring botnet-related threats 42
Box 10. Security indicators on attack traffic based on Akamai 43
Box 11. Security indicators based on IT vulnerability databases 44
Box 12. Security indicators on SSL certificates and secure servers based on Netcraft 46
Box 13. Challenges in estimating the costs of cybercrime 47
Box 14. Measuring the level of skills in IT security 48
Box 15. Privacy indicators based on surveys of ICT use by households/individuals 51
Box 16. Understanding the challenges and limitations of complaint data for consumer policy making .. 54
Box 17. Privacy indicators based on privacy authority reports 56
Box 18. Privacy-related indicators based on the Consumer Sentinel Database 61
Box 19. Some anecdotal evidence related to privacy 62
Box 20. Privacy-related indicators based on reports by the AIPP 63
Box 21. Statistics on Data breach incidents 64
Box 22. Privacy-related indicators based on Tor data 65
Box 23. Indicators on children online based on surveys of ICT use by households/individuals 69

SUMMARY

The Committee for Information, Computer and Communications Policy (ICCP) is conducting work on improving measurement of the Internet economy as mandated by the OECD (2008b) *Seoul Ministerial on the Future of the Internet Economy*[1] and the OECD (2011i) *Council Recommendation on Principles for Internet Policy Making*. The latter specifically invites OECD countries to "develop capacities to bring publicly available, reliable data into the policy-making process" as a basic principle for Internet policy making.[2] Initiatives across the ICCP Committee and its sister Committee on Consumer Policy (CCP) are underway to improve the quantitative evidence base for policy making in their respective fields.

This report contributes to this larger measurement agenda by providing an overview of existing data and statistics in the fields of information security, privacy and the protection of children online. It highlights the potential for the development of better indicators in these respective fields showing in particular that there is an underexploited wealth of empirical data that, if mined and made comparable, will enrich the current evidence base for policy making. Such indicators would help identify areas where policy interventions are most clearly warranted, and can provide guidance on designing policy interventions and determining their effectiveness (see OECD, 2010d).

Starting from a broad scope covering all aspects of security and privacy, the report identifies the "low-hanging fruit", that are areas where better indicators could be developed with minimal resources as next steps. They include:

- Improving the relevance of the OECD model surveys on ICT use by businesses and households/individuals for policy makers in the areas of information security, privacy, and in particular the protection of children online.

- Improving the cross-country comparability of statistics provided by:

  - National/government Computer Security Incident Response Teams (CSIRTs) in the area of information security, and

  - Privacy enforcement authorities (privacy authorities) in the area of privacy.

The report also presents an analytical framework that, when applied to all questions of the OECD model surveys related to information security, privacy, and the protection of children online, identifies the concentration of existing indicators in specific areas, and most importantly, potential gaps for policy makers. The application of the framework highlights that the OECD model surveys on ICT use, in their current revision, concentrate on technical and social aspects, while not addressing economic aspects, which however would be important for policy makers when assessing the socio-economic impacts of potential harms. Furthermore, the report shows that the reporting of security and privacy incidents as well as their prevention stand at the core of the security and privacy related questions. However, questions on the response of businesses and households to security and privacy incidents are missing.

Security-related data collected from CSIRTs are presented and analysed. They include, among others, data on *i*) alerts and warnings; *ii*) best practices; and on *iii*) incidents handled (by type of incident). Potential indicators based on these data are identified and proposed for further discussion. These potential indicators cover technical aspects of security including threats, vulnerabilities, prevention, incidents and response. When applying the analytical framework to these potential indicators, the lack of empirical data

on response-related activities becomes apparent. In the area of privacy, the privacy authorities' annual reports provide a rich source for data. For instance, the privacy protection authorities' data stand out from other data, as they provide certain types of data relevant to the economics of personal data protection. Data collected include, but are not limited to: *i*) budget allocated; *ii*) personnel; *iii*) complaints received and addressed; and *iv*) investigations. New indicators based on these data are developed and proposed for further discussion.

Internet traffic *automatically* generates large amounts of promising security- and privacy-related data that can be collected and distributed in *real-time*. Examples in the area of information security include data on malware and botnets collected through the private sector namely through IT security firms and *honey nets*[3], that are networks of systems that emulate a set of vulnerable IT services to attract *e.g* malware (like fly-paper). Data collected can then be shared between experts and linked to each other. In the area of privacy, browser plug-ins such as *Ghostery* enable users to detect and control known Web tracking elements. Statistics on these trackers are collected and can be further analysed. All these data sets are promising, but require further assessment in order to qualify as solid evidence base for policy making.

One particular limitation persists independently of the data source used, which is the fact that not all incidents are visible to users because of a number of factors including users' technical limitations, the surreptitious nature of some privacy and security violations, or because of a lack of transparency in business practices. Therefore, only incidents that have been identified as such and fully disclosed can be measured. However, these incidents constitute only an unknown share of the total number of incidents. This has some serious implications on the significance of statistics related to information security, privacy and the protection of children online. For example, a decrease in the number of malware infections may be an indication of *i*) the success of security measures to prevent infections; *ii*) a decreasing ability to detect malware; *iii*) a decreasing number of malware produced; *iv*) more targeted attacks; and/or *v*) the number of devices increasing faster than the number of infections.

To exploit the full potential of the data and statistics presented in this report, a sound assessment of major influencing factors is therefore necessary. This not only calls for linking and correlating available data on information security, privacy and the protection of children online with each other, but also linking these data with other databases available in the OECD such as the OECD Broadband Portal and the OECD Patent Database. In doing so, the collected data and statistics can be cross-validated and at the same time provide a more holistic view on information security, privacy and the protection of children online. Linking these data sources would thus take advantage of the unique position the OECD provides for discussions on information security, privacy and the protection of children online.

INTRODUCTION

"If you cannot measure it, you cannot improve it."
Lord Kelvin (Sir William Thomson)

Information security[4] and privacy challenges continue to increase as individuals, businesses, and governments are shifting large parts of their daily activities to the Internet. Malware are reported to be spreading at high rates, increasing the risks of compromising information infrastructures (see OECD, 2009; van Eeten *et al*., 2010).[5] Advances in transborder data flows of personal data as well as big data storage and analytics amplify the risk of misuse of personal data, and challenge the application of privacy protection regulation (see OECD, 2010a).

At the same time, information security and privacy issues have reached a tipping point where policy makers can no longer neglect their implications on innovation, economic growth, and prosperity. The horizontal project on the "Economics of Personal Data", for example, highlights the value of personal data and its contribution to innovation as a "New Source of Growth" in sectors as diverse as health care, finance, energy, and marketing (see OECD, 2011a; OECD, 2011b).[6] Likewise, the work on "National Cybersecurity Strategies" reveals that OECD governments now recognize that the Internet has evolved from a *useful* platform for e-commerce and e-government to an *essential* infrastructure for the functioning of the society, making information security a "national security" concern (see OECD, 2011c).

These evolving challenges and opportunities, and the increasing effects privacy and information security policies have on trust, innovation and growth across the economy, call for improving the evidence-based for security and privacy policies for the following three reasons: first, to identify where policy interventions on privacy and security are warranted; second, to design better security and privacy policies, thereby limiting as much as possible unintended consequences and thus costly mistake; and third, to better assess the effectiveness, benefits and costs of existing and proposed security and privacy policies. In the context of a still fragile recovery and government budget deficits, these arguments become even more compelling.

Building the evidence base

Most policy makers and analysts consider the concept of evidence-based policy self-explanatory. Therefore, an explicit definition for "evidence-base policy" is rarely being provided. As Marston and Watts (2003) explain, "it is difficult to imagine anyone arguing that policy should be based on anything but the best available evidence". Definitions, when available, often stress "the systematic appraisal and review of empirical research findings" in policy making as the main characteristic of evidence-based policy (see Sanderson, 2002; Marston and Watts, 2003; Banks, 2009).[7] Evidence-based policy making therefore stands in contrast to policy making that is mainly driven by intuition, opinions, and ideologies, "or, at best, theory alone" (Banks, 2009, see also Davies, 2004).[8]

The information constituting the evidence base can originate from different sources, such as empirical research and statistics, policy evaluation, statistical modelling, and expert knowledge (see Nutley *et al*., 2002).[9] This information can be either *quantitative,* such as statistics and economic models, or *qualitative,* such as expert knowledge and case studies. In any case, information must be gathered and approved *systematically* and based on *transparent criteria* and *methodologies* in order to qualify as strong evidence for policy making.

In this respect, evidence-based policy making is by no means new to the OECD Working Party on Information Security and Privacy (WPISP). WPISP has been providing policy makers with evidence on information security and privacy since its early work. However, most work in the past has been based on qualitative rather than on quantitative evidence, with few exceptions, such as the OECD (2009) report on "Computer Viruses and Other Malicious Software". This is most likely due to the challenges associated with the development of empirical datasets and quantitative indicators in the field of privacy and security as stressed by the following reports, which also call for better indicators:[10]

- The OECD (2005a) report on "The Promotion of a Culture of Security for Information Systems and Networks" highlights the lack of metrics and benchmarks to assess the overall effectiveness of national information security policies.

- The OECD-APEC (2009) report on "Computer Viruses and Other Malicious Software" concludes that international co-operation for addressing malware should be supported and enhanced by accurate and quantitative measurement of the problem.

- The OECD (2012a) Council Recommendation on the Protection of Children Online encourages governments to support evidence-based policies for the protection of children online by facilitating the further development of a robust empirical and analytical basis.

Empirical data, statistics, and indicators

Indicators are frequently used as quantitative evidence in policy making. They are a means to measure, indicate and point out to the past, current, and predicted or targeted elements of the subject to be measured. Because they are used to measure, they are sometimes also referred to as "*metrics*" (see *e.g.* broadband metrics). Indicators typically convey some theory. For example, the unemployment rate is an economic indicator defined as the ratio between unemployment and labour force, because the theory suggests that the labour force is the relevant reference. Depending on the theory in mind, it could be *e.g.* working aged population, total population, etc.

When empirical data are available, it becomes possible to calculate a single measure of a data attribute of interest, such as the sum and the average of the attribute. This single measure is called a *statistic* of the empirical data sample. For example, when collecting data on security incidents, a statistic like the total

number of incidents or the average number of records stolen per data breach can be calculated. These statistics can then be used to create indicators based on some theory. Empirical data are typically generated from *i*) surveys; *ii*) activity reports; and *iii*) the Internet. These sources are presented in more detail in the following sections.[11]

Surveys

Surveys (or polls) are one of the most frequent sources for empirical data used for policy making. They are based on questions asked to people (*i.e.* the sample population). Their goal is to learn about certain attributes of the population based on a sample of this population through statistical inference. In order for the inference to be correct, the sample needs to be representative; that is it has to reflect the main characteristics of the population of concern. National statistics offices, for example, put great effort in the design of their national surveys such as the *Current Population Surveys* (CPS) in the United States and the *Community Surveys on ICT Usage* in the European Union to assure the representativeness of the population sample.

The biggest advantages of surveys are the following (for a comprehensive discussion on the use of surveys for policy making in the area of consumer protection see OECD, 2011g):

- Surveys allow a systematic collection of comparable data across different groups of individuals, firms, and countries, if designed and implemented accordingly (see OECD model surveys on ICT use).
- Surveys can capture qualitative information such as those related to trust.
- Last but not least, surveys are flexible, meaning that the set of information collected can be adjusted according to current policy needs.

However, surveys have drawbacks, which should be taken into account when undertaking them and when interpreting their results. Firstly, the operation of a survey can be costly and time consuming. Depending on the characteristic of the population, the size of the sample must be significantly large to be representative.[12] However, not enough individuals or firms may be motivated to participate. Furthermore, surveys tend to confirm existing preconceptions and fail to bring up new insights (OECD, 2011g). The most severe drawback, however, is that surveys assume that the answers provided by respondents are correct. Research has shown, however, that individuals may sometimes not be willing or able to answer the surveys correctly. This can be because respondents either *i*) consider the question asked too sensitive; or *ii*) do not have the necessary skills to understand and answer the question correctly. This is a major issue when it comes to surveys on security in particular, where the technical requirements to answer questions correctly can be either too high for some individuals or considered too sensitive to be answered honestly. In some cases, users simply cannot know if an incident occurred.[13]

Activity reports and related data

Activity reports are another common source for empirical data. Typically, they are published by an organisation periodically, *e.g.* annually, quarterly, or monthly, either because of legal obligations or on a voluntary basis. Activity reports are intended to give stakeholders information about the organisation's routine work and its current conditions. Examples of activity reports are firms' annual reports including their financial statements and activity reports published by privacy enforcement authorities and Computer Security Incident Response Teams (CSIRTs).

One of the biggest advantages of using activity reports as a source of data is the periodical nature of the published data. This allows the building of a time series from the reported data, for either short- or long-term trend analysis. For example, revenues published in a firm's annual reports can be collected to analyse trends in revenues' development over years.

However, there are also some challenges associated to the use of activity reports. First, the rules of how to report may differ from one organisation or country to another, making reported data sometimes very difficult to compare across organisations and countries in contrast to survey data. Furthermore, sometimes even within the same organisation, data reported across different periods can also be difficult to compare. This can be due to changes in reporting rules (*e.g.* change in legislation) or, for instance, due to merging and acquisition of organisations, in which case the organisation can hardly be compared even with itself in previous years.

Internet-based statistics

The Internet is a rich source of data. When it comes to measuring Internet-related activities, Internet traffic can provide big data sets for analysis. It is therefore not surprising that the Internet has already been considered a valid source for providing the evidence for policy making by the United Kingdom Strategic Policy Making Team (SPMT, 1999) (see also Davies, 2004). Recent OECD (2010b) work on "Internet-based Statistics" is evaluating how the Internet can be used more systematically as an additional source for national statistics.

One of the strengths of Internet-based data is that the data is *automatically* generated and can be collected and distributed in *real-time* via the Internet. Thus Internet-generated data collection tends to be less costly, compared to surveys in particular. For example, data collected on malware, be it through antivirus or firewall solutions, can be communicated directly to providers of these tools and made available to users and researchers in real-time via the providers' web sites.

But there are also some challenges associated with Internet-generated data. In some cases, the information collected may only reflect the situation of particular users of the providers' tools, and thus may only permit limited conclusions to be drawn from the data in respect of the entire population. Internet-based data should therefore be cross-validated using other sources such as surveys and reports. Last but not least, there is a risk that data collected over the Internet could violate the privacy of Internet users. Therefore, identifiers, such as IP-addresses, are usually anonymized or aggregated before further analysis is done.

Benefits and limitations in measurement

Besides the issues associated to each data source, there is an additional challenge, which is linked to the question of measurability in general. Because of the illegal nature of privacy and security violations, not all incidents appear in *e.g.* national statistics including even crime statistics. One must be aware of the following fundamental limitations of measuring privacy and security incidents: only incidents that have been identified as such can be measured, and such incidents constitute only an unknown share of the total number of incidents. This has some serious implications on how to interpret numbers of privacy and security incidents. For example, a decrease in the number of malware infections may be an indication of *i*) the success of security measures to prevent infections; *ii*) a decreasing ability to detect malware; or just for *iii*) a decreasing number of malware produced by malicious users.

Therefore, indicators presented in this report are best interpreted in context, in particular when linked to other datasets. This not only includes linking data sources on privacy with each other as well as data on security with each other, but also linking data from both areas together. The latter would allow, for

example, a better understanding of how privacy protection measures may affect security and *vice versa*. Furthermore, by linking data on security and privacy with other OECD databases, the impact of information security and privacy policies on *e.g.* innovation and growth in the Internet economy can be better assessed (see Box 1 for potential databases). Linking these databases would thus take advantage of the unique position the OECD provides for discussions on privacy and security policies.

That said, measuring the visible side of the phenomenon still remains very useful to understand trends in, and to improve the ability to handle the risks for, privacy and security. Not only can data on the visible side act as *proxy* for the overall phenomenon (reasonable assumptions will have to be made still), but a better ability to measure privacy and security incidents will lead to better indicators which will lead to better security and privacy policies. This is because better measurements require better monitoring systems, which in turn leads to improved security and privacy.[14]

Overall, providing evidence for policy making and a mean to set clearer policy objectives and to monitor their effectiveness are among the most important roles of indicators. This is consistent with the 2008 Seoul Ministerial Declaration,[15] which highlights that improved indicators are needed both for developing better policies on information security and privacy and for assessing their effectiveness on a regular basis (see OECD, 2008). It is also in line with the OECD (2011i) *Council Recommendation on Principles for Internet Policy Making*, which calls to "develop capacities to bring publicly available, reliable data into the policy-making process" as a basic principle for Internet policy making.[16] Furthermore, indicators can provide a basis for improving awareness in security and privacy, as encouraged, for example, by the OECD (2002) *Security Guidelines*[17] and the OECD (2003) *Privacy Online: Policy and Practical Guidance.*[18] Thus, the indicators discussed in this report will not only help increase the efficiency and effectiveness of policies, but they can also be used to attribute responsibilities and raise accountability and awareness among all stakeholders.

Box 1. Linking security and privacy data with existing OECD databases

By linking collected empirical data on privacy and security with existing OECD databases, powerful indicators can be developed which can provide a holistic view on security and privacy. The following list is an incomplete list of databases that could be combined with data collected in this work.

1. **The OECD Broadband Portal** provides access to a range of broadband-related statistics. Indicators provided reflect the status of individual broadband markets in the OECD in five main categories: *i*) penetration; *ii*) usage; *iii*) coverage; *iv*) prices; *v*) services and speeds. By linking data on privacy and security to the broadband portal data, security and privacy indicators can be developed that reflect the current status of individual broadband markets.

2. **The OECD Information Technology Database** is a database compiled from annual reports, SEC filings and market financials of the top information communication technology (ICT) firms. It includes data on revenues, R&D expenditure, employment, net income, and net cash. This database can provide insights on the market for IT security, privacy protection, and children online protection solutions. But it can also be used to analyse the impact of security and privacy violation on spending on R&D, employment and revenue of Internet-related firms.

3. **The OECD Patent Database** was set up to develop patent indicators that are suitable for statistical analysis and that can help address science and technology policy issues. The Patent Database covers data on patent applications to the European Patent Office (EPO), the US Patent and Trademark Office (USPTO), patent applications filed under the Patent Co-operation Treaty (PCT) that designate the EPO, as well as Triadic Patent Families. In the context of this work, this database can be used to analyse innovation in the area of security and privacy.

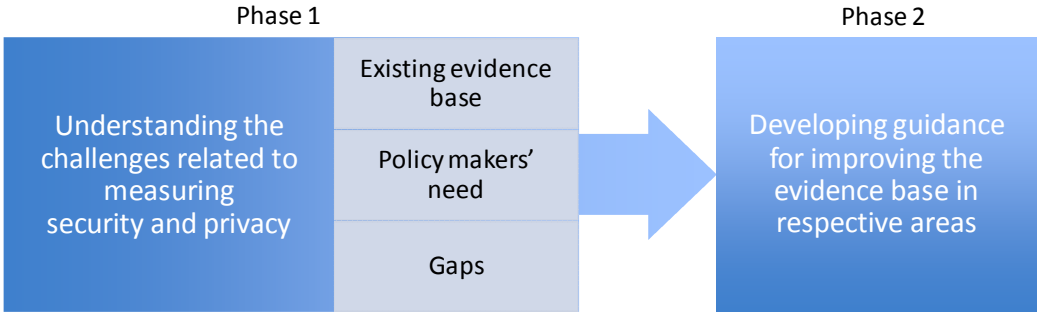
Source: OECD

Objectives and methodology

This work aims to develop the evidence base for policy making in the areas of security and privacy, including for the protection of children online. Previous OECD work in this area had a limited scope, focusing, for instance, on data provided by national statistical offices such as work by the Working Party on Indicators for the Information Society (WPIIS) (see OECD, 2005b; 2007), or on e-government such as the proposal by the WPISP in 2008 to work on security and trust indicators.

Moving beyond the limited scope increases the complexity, but also the chance, for a better understanding of the quantitative dimension of information security and privacy. In order to cope with the complexity, a multi-phase-approach is proposed *Phase one* aims to understand the overall challenges related to measuring information security and privacy: starting from a broad scope covering all aspects of security, privacy, and the protection of children online (*i*) the existing empirical data and statistics will be identified and assessed in order to provide a comprehensive picture of the potential gaps between the need for evidence for policy making and existing data. *Phase two* will focus on potential areas for improving the existing evidence base in respective areas identified in this report as the "low hanging fruit". Figure 1 summarises the phases of the project.

Figure 1. Phases of the project



This report is part of phase one and focuses on understanding the overall challenges related to measuring information security, privacy, and the protection of children online. Its primary objective is to provide a *systematic* overview of the data available from national statistical offices, other government agencies, and non-government organisation (NGOs). Collected data are discussed in terms of their comparability, reliability, and availability over time. The second goal of this paper is to highlight potential gaps between policy makers' needs and the existing evidence base. Particular attention will be paid to potential "low hanging fruit", *i.e.* areas where comparable indicators could be derived with minimal efforts. This report, however, does not provide a discussion on the relevance of these data and statistics to current policy makers' need, which will rather follow as a next step of this project.

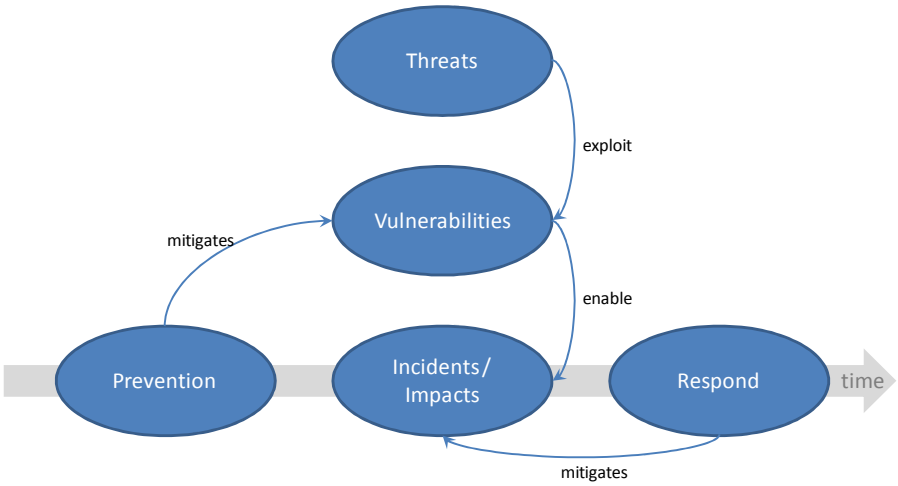
An analytical framework has been developed that classifies statistics and empirical data by the following three criteria:

Threats, vulnerabilities, prevention, incidents/impacts, and response are the object to be measured in the area of security, privacy, and the protection of children online. Threats, vulnerabilities, and incidents/impact are *risk assessment* factors, with risk being defined as the potential of threats to exploit vulnerabilities leading to detrimental incidents/impacts. Prevention and response are measures taken before and after an incident respectively, and they are part of *risk management*. The relationship between these factors is presented in Figure 2.

- **Social, economic, and technical perspectives** describe the type of indicator to be used for measurement. *Social indicators* are indicators that measure *e.g.* the behaviour of individuals or the society. *Economic indicators* measure the costs and benefits (in monetary values). All other indicators that are not social or economic are *technical indicators*.

- **Governments, businesses, individual and households** are the *actors* that may have different incentives and roles to play. The categories of actors can be further differentiated in subgroups depending on the policy need, such as small and medium enterprises (SMEs) and large enterprises in the case of businesses, parents and children in the case of individuals, and regulators such as privacy authorities and the public administration in the case of government. Other actors could also be included such as criminals or wrongdoers to cover the measurement of fraud and illegal activities (*e.g.* market for malware).

Figure 2. The relationship between risk factors



The matrix in Table 1 is used to classify statistics and data related to governments, businesses, individuals and households, respectively. Each cell within the matrix represents one potential measurement point and shows where existing indicators are concentrated. As an illustration, the number of bot-infected machines provides an indication of the security threat from a technical perspective (A); In the area of privacy, the number of means to collect and analyse personal data (*e.g.* big data analytics) is also considered a technical threat (B). The number of individuals filing a complaint to a privacy regulator measures (the perception of) privacy incidents and impact from a social perspective (C); the share of parental control software used indicates the level of awareness of parents regarding online threats to children from a social perspective (D) as well as prevention measures from a technical perspective (E).

Table 1. Matrix for classifying indicators on information security and privacy

		Risk assessment			Risk management	
		Threats	Vulnerabilities	Incidents/ Impact	Prevention	Response
Perspective	Social	D		C		
	Economic					
	Technical	A, B			E	

Source: OECD

Structure

This report is divided in four sections, focusing on available data and statistics in the area of *i*) security, *ii*) privacy, and *iii*) the protection of children online, respectively, as well as on *iv*) identifying the policy makers' needs and the gap analysis. Each of the first three sections is divided into four subsections, with the first three covering indicators and empirical data provided by *i*) official statistics agencies, *ii*) other government agencies, and *iii*) the private sector. Data provided by official statistics agencies, other government agencies, and the private sector are described briefly as follows:

- **Official statistics agencies:** Statistics provided by national statistical agencies are considered to be the most reliable. This is because "the value of this information is rooted in the traditional strengths of national statistical offices which include: transparent and well-defined methodologies, integrated conceptual frameworks, large sample sizes and relatively high response rates" (OECD, 2005b). Indicators provided by official statistics agencies are therefore considered *official statistics*. For the development of security and privacy indicators, "the main approach of official statistical agencies [is still] to gather data from surveys of households and businesses on the use of ICT" (OECD, 2005b).[19] This comes along with the limitations discussed in the previous section. On the other hand, statistics provided on the perceived trust barriers to Internet use are still unique and one of the rare sources for trust-related indicators.

- **Other government and public agencies:** A growing body of statistics comes from a range of government and public agencies, which publish data relevant to inform questions on privacy and security, mainly through activity reports usually on an annual or monthly basis. Among the most promising data are activity report and related data published by *privacy protection authorities (privacy authorities)* in the area of privacy, by *computer emergency response teams (CERTs)* in the area of security, but also *consumer protection authorities* in areas affecting consumers. Other promising sources include law enforcement authorities (LEAs) publishing e-crime statistics as well as reports of consumer protection agencies. Besides these data that are generated by the routine work and published through activity reports, some agencies also engage in surveys, whose results are either published in their annual reports, or on their websites. Data provided by these government agencies are sometimes referred to as *semi-official data* because they do not guarantee the rigorousness and statistical strengths national statistical offices provide.

- **The private sector:** The private sector, including commercial as well as not-for-profit organisations, are an important source for data. One reason is that the private sector includes the group of bodies that collects and provides Internet-based statistics most frequently. This consists of data collected on *e.g.* malware (through *e.g.* antivirus software, web crawlers, and honey nets) and privacy violations (through *e.g.* web browsers tracking unsolicited cookies). A significant amount of data provided by NGOs is also generated through surveys and activity reports. The biggest challenges associated with these data are due to the methodologies employed, which sometimes lack the transparency and clear definitions that are required.

Finally, indicators developed based on the data surveyed are presented in boxes for further discussion. A short analysis is included respectively.

INFORMATION SECURITY

This section focuses on indicators and empirical data on security. It starts by assessing indicators provided by *i*) official statistics agencies, in particular the *OECD model surveys of ICT (information, communication technology) use*. It then looks at statistics and empirical data published by *ii*) other government and public agencies, in particular by national and government *Computer Emergency Response Teams* (CERTs), *law enforcement agencies* (LEAs) and consumer protection agencies. The next section then assesses data provided by *iii*) non-governmental organisations. These include in particular data provided by *IT security tool providers*, *vulnerability databases*, *network services and equipment operators*, *certificate authorities*, *honey pot operators* and *consulting and audit companies*. Where enough data are available, the matrix presented in Table 1 will be applied for classifying existing and potential indicators.

Official statistics agencies

This section will present statistics available at official statistics agencies. It will in particular discuss the methodology and scope applied for data collection as proposed by the *OECD model survey of ICT use*. Finally, it will apply the analytical framework presented in Table 1 to show the concentration of existing indicators in specific areas and to highlight potential gaps for policy making.

OECD model survey of ICT use by businesses

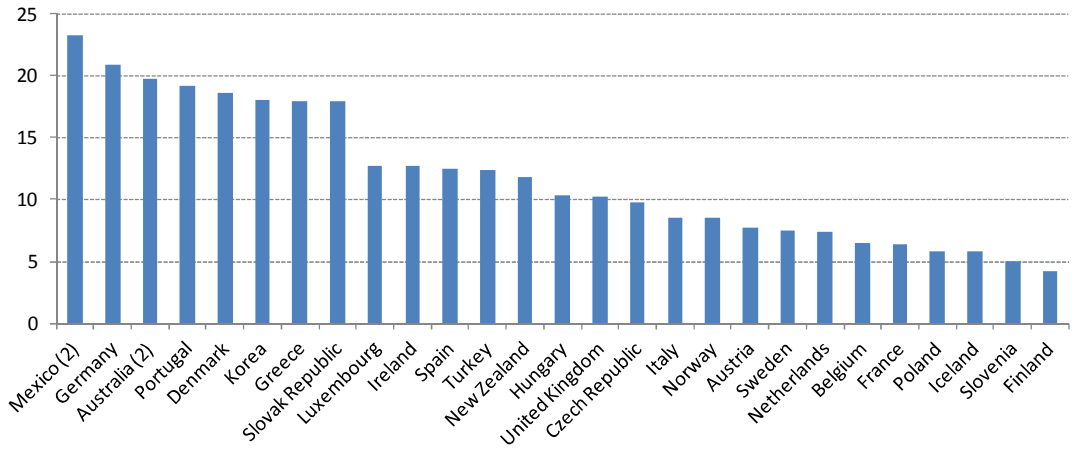
The *OECD model survey of ICT use by businesses* includes a number of questions that deal with the topic of IT security and privacy in the context of: i) trust in the online environment, ii) e-business, iii) digitised products; and (iv) e-government from a business perspective (see Box 2 for some examples). These questions are usually related to firms' encounters with IT security incidents, their origins or consequences (see OECD, 2011d).

The OECD model survey was finalised by the OECD Working Party on Indicators for the Information Society (WPIIS) in 2001, updated in 2005 in co-operation with the WPISP, and is currently under revision to improve harmonisation with member country ICT use surveys and to take into account current areas of high policy relevance (OECD, 2011d). Eurostat, the statistical office of the European Union, and a number of member countries have been working with the OECD in developing and revising the model survey. Eurostat, in particular, contributed through its *Community survey on ICT usage in enterprises*, which is mandatory and implemented according to regulation (EC, 808/2004).

Box 2. Security indicators based on surveys of ICT use by businesses

The following indicators are few examples created on the base of official surveys on ICT use by businesses. Figure 3, for example, shows that the share of businesses with 10 or more employees that have encountered IT security incidents that resulted in the destruction or corruption of data due to infection or malicious software or unauthorized access in 2010 was roughly between 5% and 25%. Figure 4, as another example, shows that the share of businesses using a secure protocol for the reception of orders via Internet is around 20% in the EU.

Figure 3. Businesses that have encountered IT security problems[1] in 2010
Percentage of total businesses

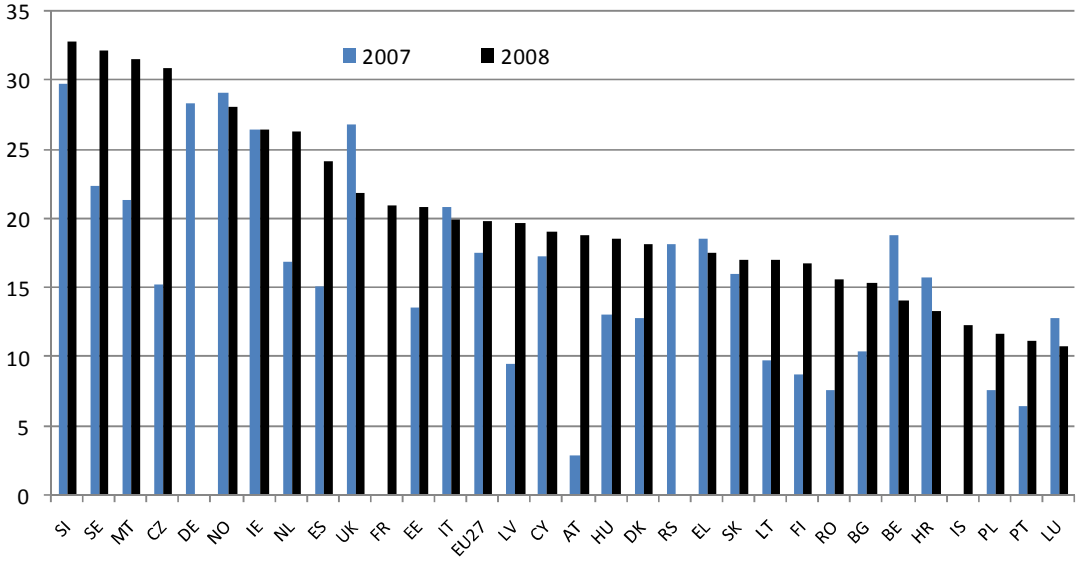


Note: (1) "IT security problems" is defined in general as security incidents that results in destruction or corruption of data due to infection or malicious software or unauthorised access. For Japan, Korea and Mexico data refer to virus, trojan or worm only.

(2) 2008; For Australia: Data refer to any IT security problems; For New Zealand: Includes threats such as virus, trojans or worms, attacks resulting in Denial of Service, or unauthorised access to business computer systems or data.

OECD, ICT database and Eurostat, Community survey on ICT usage and e-Commerce in businesses, 2008.

Figure 4. Businesses using a secure protocol for the reception of orders via Internet in 2008
Percentage of total businesses

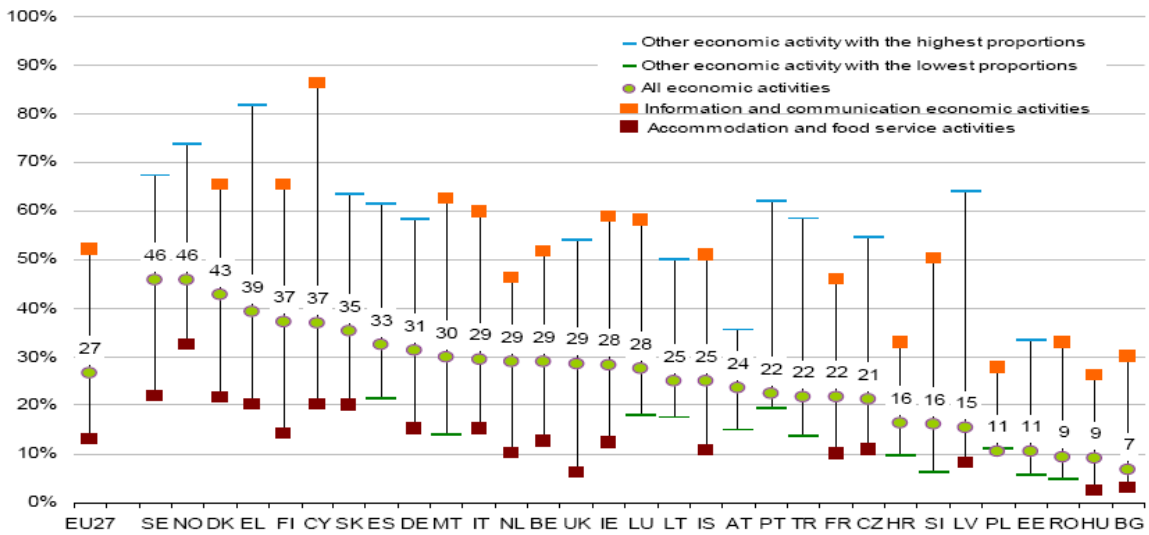


Source: Eurostat, Community Survey on ICT usage in businesses, 2008

Box 2. Security indicators based on surveys of ICT use by businesses (cont.)

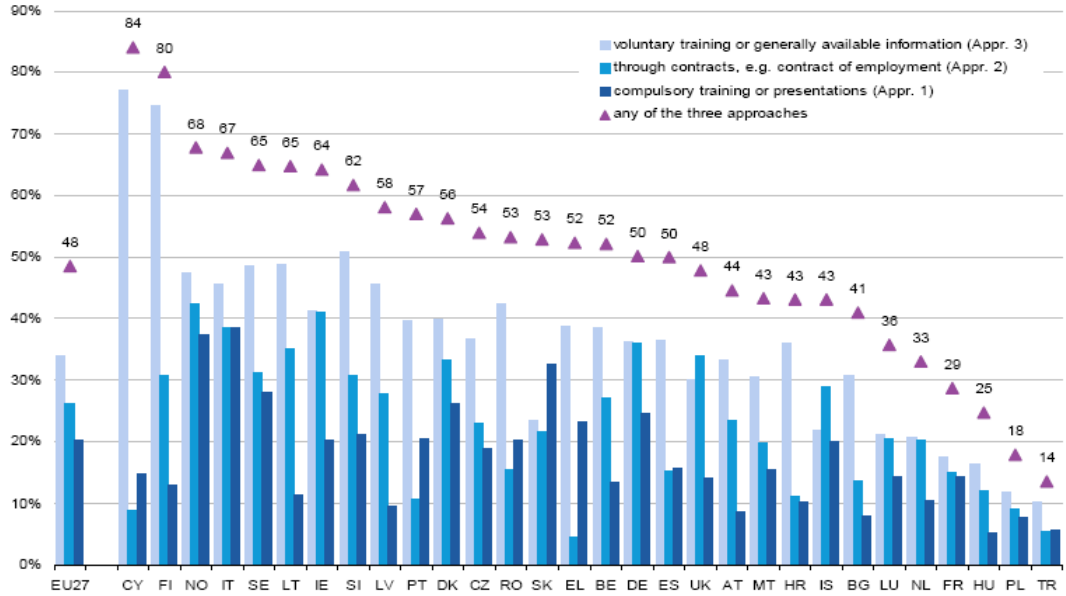
Figure 5 shows the proportions of enterprises having a formally defined ICT security policy. It illustrates that Sweden, Norway and Denmark have the highest proportions of enterprises having a formally defined ICT security policy with a plan for regular review (with 46 %, 46% and 43% of all enterprises respectively). Figure 6 highlights that voluntary training or use of generally available information have been most frequently used by enterprises to make staff aware of their ICT-related security obligations.

Figure 5. Range of the highest-lowest proportions of enterprises having a formally defined ICT security policy with a plan for regular review, by country and economic activity, January 2010 (% of enterprises)



Source: Eurostat, Community Survey on ICT usage in businesses, 2010

Figure 6. Approach adopted by enterprises to make staff aware of their obligations in relation to ICT security, by country, January 2010 (% of enterprises)



Source: Eurostat, Community Survey on ICT usage in businesses, 2010

Methodology

The OECD model survey of ICT use by businesses encourages participating countries to follow a set of best practices in order to prevent inconsistencies between member countries. It includes recommendations on *i*) how to minimize sampling and non-sampling errors; *ii*) survey vehicles; *iii*) collection techniques; *iv*) statistical units, their selection and weighting, and (*v*) survey frequency and reference period/date. These recommendations are presented in detail in Annex 5.A1 of OECD (2011d).

Scope and coverage

The survey covers businesses from the private and public sectors that are operating in the country conducting the survey. General government organisations are excluded and most OECD countries also exclude non-employers (OECD, 2011d). The OECD model survey also recommends including only businesses that have *10 or more employees* in order to be consistent with Eurostat surveys. Furthermore, because ICT intensiveness varies by industry, efforts have been made to use reasonably consistent industry classifications leading to the following *industry scope* (see Annex 5.A1 in OECD, 2011d): *i*) manufacturing, *ii)* construction, *iii*) wholesale and retail trade, *iv*) repair of motor vehicles, motorcycles, *v*) household goods, *vi*) hotels and restaurants, *vii*) transport, storage and communications, *viii*) financial intermediation, *ix*) real estate, renting and business activities; and *x*) recreational, cultural and sporting activities.

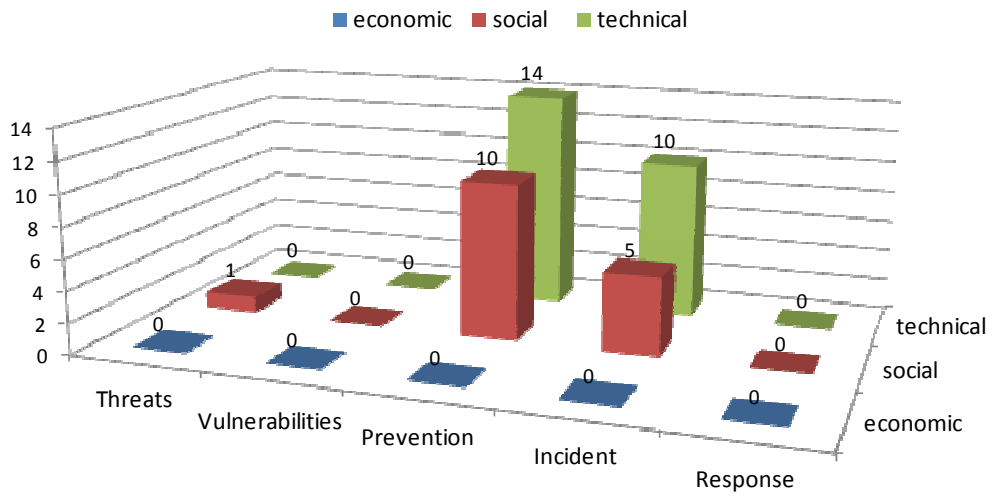
Issues have been raised by member countries, regarding the limitations of such surveys in the field of security given the risk that businesses will either not answer such questions or will understate the extent of any problems. As a result, questions on IT security incidents were reduced to attacks by malware (OECD, 2011d).

Gap analysis

Overall, 34 different questions related to security have been asked to businesses through the OECD model survey between 2007 and 2010. Most questions have been asked in 2010 with a special IT security module being introduced in the OECD model survey.

By systematically mapping all questions related to security of the OECD model survey to the framework presented in the introduction, and using the matrix in Table 1, the concentration of existing indicators in specific areas can be highlighted, and most importantly, potential gaps can be identified. Figure 7 shows the distribution of questions over the fields of the analytical matrix.

Figure 7. Number of questions related to security in the Eurostat Community Survey on ICT usage in businesses, by type of indicator



Source: OECD based on Eurostat, Community Survey on ICT usage in businesses

The following general observations can be made:

1. Questions related to security in the OECD model survey and the community survey of ICT use by businesses focus on the technical and social aspects of IT security, with a particular weight on incidents and specific prevention measures such as the use of firewalls and antivirus software. This includes, for example, all questions related to *e.g.* business policies to increase security awareness as well as to questions related to security incidents.

2. Potential gaps appear in areas related to security threats, vulnerabilities and response measures as well as in regards to economic indicators. For example:

   a. The OECD model survey and the community survey in particular do not include questions related to measures undertaken *after* a security incident (see *response*).[20] The following questions related to response measures could thus be added to the survey:

      1. What solutions have been chosen to eradicate the infection: *i*) removing malware artefacts, *ii*) restoring from backup, and/or *iii*) rebuilding the relevant systems?

      2. Have *i*) CERTs, *ii*) law enforcement, or *iii*) other external organisations been contacted after a security incident has been detected?

   b. Furthermore, questions related to vulnerabilities and threats such as the following are missing and could be added to the survey: Does the company regularly assess its IT vulnerabilities and threats?

   c. Finally, these surveys do not provide economic indicators, such as investments by businesses in the area of security or on costs of security incidents.

OECD model survey of ICT use by households/individuals

The *OECD model survey of ICT use by households/individuals* includes a number of questions that deal with IT security, privacy, and trust as barriers for households and individuals (see Box 3 for some examples). This survey was finalized by the WPIIS in 2002, updated in 2005 in co-operation with the WPISP, and is currently under revision to improve harmonisation and to reflect current areas of high policy relevance. Eurostat and a number of member countries have been working with the OECD in developing and revising the model survey.

Methodology

The methodology of the OECD model surveys of ICT use by households/individuals is similar to the OECD model surveys for businesses, with participants encouraged to follow a set of best practices in order to prevent inconsistencies between member countries. These recommendations are presented in detail in Annex 6.A1 of OECD (2011d) and include recommendations on *i*) how to minimize sampling and non-sampling errors; *ii*) collection techniques; *iii*) statistical units; their selection and weighting; and *iv*) survey frequency and reference period/date.

Scope and coverage

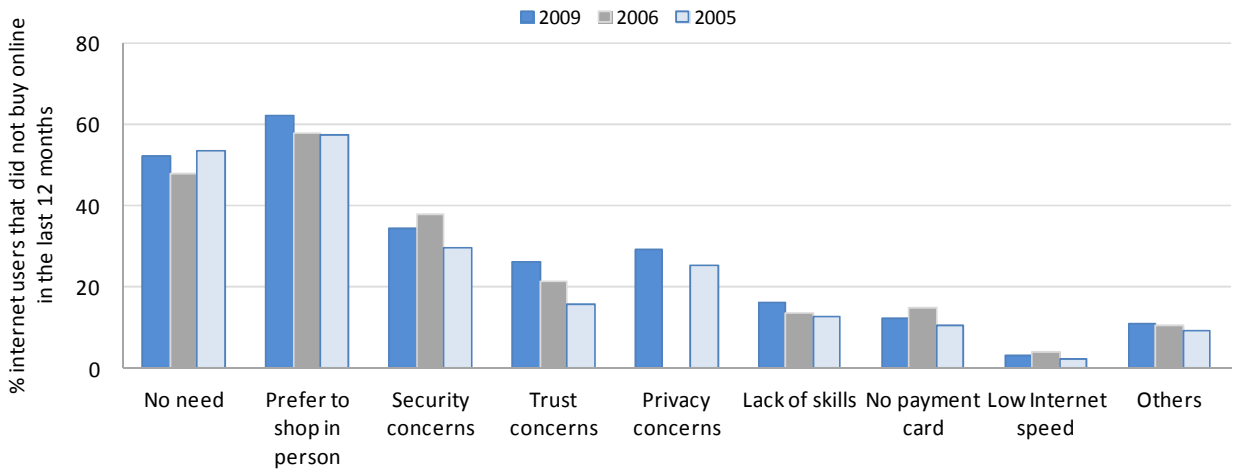
The survey covers individuals and households. The scope of individuals is limited by age and is currently set to 16-74 years. Aside from *age*, other characteristics for individuals include *highest education level received*, *employment status*, and *gender* and *occupation*. Households are characterised by their size and type (those with and without children under 16).[21]

As for the business model survey, experts from Eurostat and other national statistics agencies highlighted the problem of asking individuals about IT security. The reason provided was that respondents were unlikely to be able to respond to such technical questions, the only exception being whether individuals regularly back up important files. As a result, the model survey is therefore limited to home use only as this is the environment about which users are likely to know most and over which they have most control in contrast to material at work or at school (see OECD, 2011d).

Box 3. Security indicators based on surveys of ICT use by households/individuals

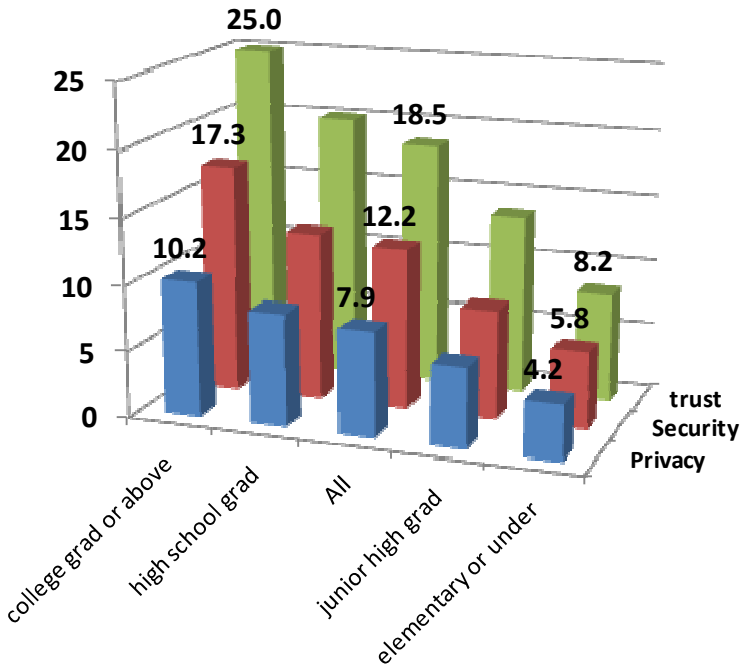
The following indicators are some examples that have been created based on the OECD model surveys of ICT use by households/individuals. Figure 8 and Figure 9, for example, show that security concerns are perceived as a significant barrier for e-commerce in the EU and Korea, respectively. In Korea, the data reveals in addition that the greater the level of education, the more trust, security and privacy become an issue.

Figure 8. Reasons for Internet users not buying online in the EU countries, 2009
Percentage of individuals with Internet access that did not buy on-line in the last 12 months



Source: OECD based on Eurostat, Community Survey on ICT usage in households and by individuals

Figure 9. Reasons for Internet users not buying online in Korea, 2008

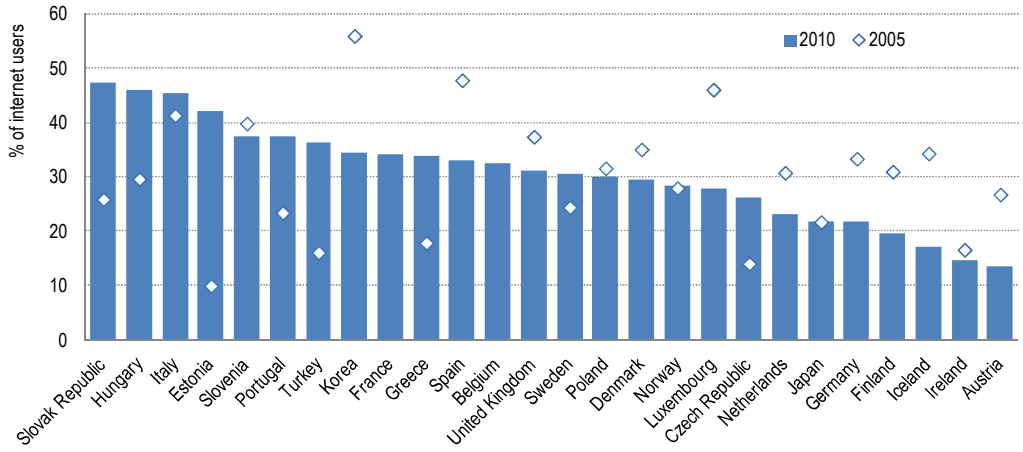


Source: OECD based on NIDA.

Box 3. Security indicators based on surveys of ICT use by households/individuals (cont.)

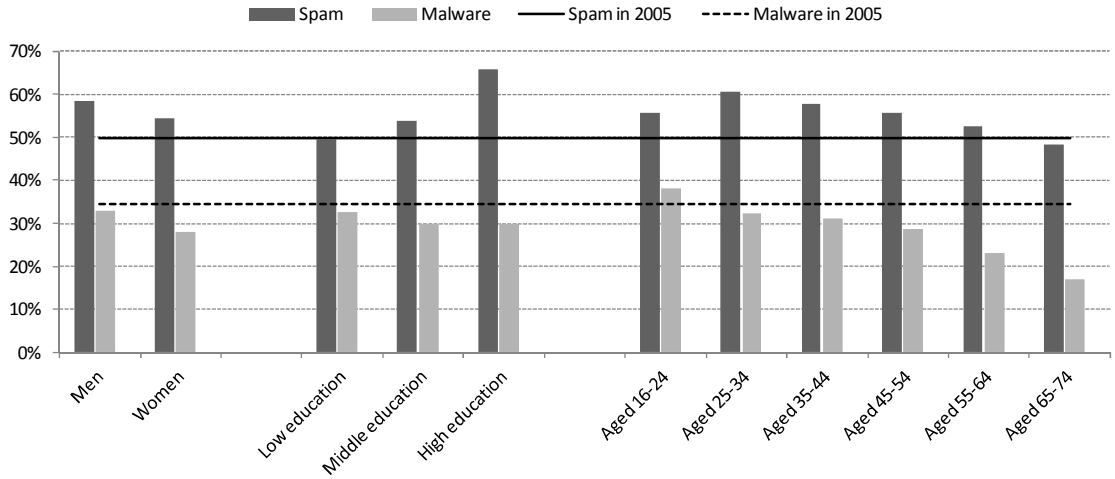
Figure 10, as another example, shows the share of individuals among all internet users, who have encountered a computer virus in the last year by using the Internet. It highlights in particular that the share has increased significantly compared to 2005 in some countries like Estonia, Turkey, Greece, and Slovak Republic, while it has decreased in others like Korea, Luxembourg, Iceland, and Austria. Figure 11, finally, shows the share of individuals in the EU suffering from virus attacks or receiving spam by demographic factors and Internet connection. It highlights, for example, that individuals with higher education are more likely to feel negatively affected by spam.[1] This confirms trends observed in Korea in 2008. It is interesting to note that there are a number of potential reasons other than indirect factors such as education level why one individual may receive more spam than another individual including: choice of email address, use of e-mail address, whether or not (and to what extent) the email address is "published" on the Internet.

Figure 10. Internet users who have encountered a computer virus in the last year by using the Internet, 2010 or latest



Source: OECD, ICT database and Eurostat, Community Survey on ICT usage in households and by individuals.

Figure 11. Internet users in the EU27 suffering from virus attacks or receiving spam, 2010
Percentage



Note: Spam and malware in 2005 refer to the share of Internet users affected by spam and malware in 2005.

Source: OECD, ICT database and Eurostat, Community Survey on ICT usage in households and by individuals.

Gap analysis

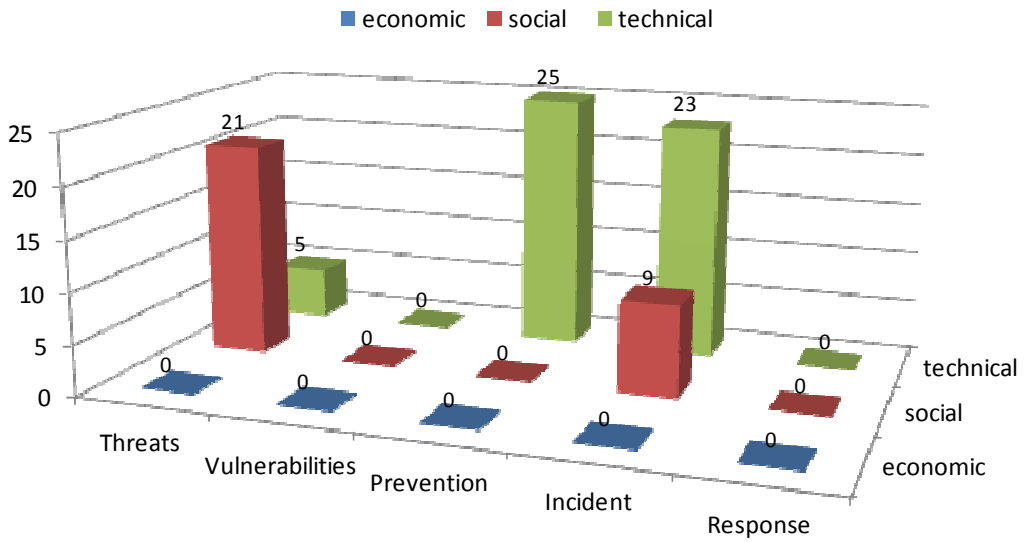
Overall, 73 different questions related to security have been identified in the Community survey. These questions have been asked through surveys taking place between 2003 and 2010, with some questions being repeatedly asked over the years and the large majority of questions asked in 2010 as a result of the introduced IT security module.

By systematically mapping all questions related to security of the Community survey to the framework as done in the previous section, the concentration of existing indicators and gaps in specific areas can be highlighted (see Figure 12). The following general observations can be made:

As is the case for the business survey, questions related to security in the OECD model survey as well as in the Community survey on ICT use in households and by individuals tend to focus on the technical and social perspective of IT security, but with a particular weight on prevention measures, incidents, and threats. This includes, for example, all questions related to *e.g.* security tools installed as prevention measures, incidents related to computer virus infections, and concerns preventing the use of the Internet.

1. Potential gaps appear in areas related to security vulnerabilities, response measures as well as economic indicators. The Community and OECD model survey do not include questions related to *e.g.* measures undertaken *after* a security incident or about the perceived vulnerabilities. Furthermore, these surveys do not provide any economic indicators, such as investments by individuals made in security measures or costs of security incidents. These types of question could be considered for the current revision of the OECD model surveys.

Figure 12. Number of questions related to security in the Eurostat Community Survey on ICT usage in households and by individuals, by type of indicator



Source: OECD based on Eurostat, Community Survey on ICT usage in households and by individuals

Other government and public agencies

A fast growing number of security-related statistics and empirical data come from a range of government agencies other than national statistical agencies. They usually publish their statistics and empirical data through activity reports on a periodic basis (usually annually or monthly). The following sections analyse statistics and data published by: *i*) Computer Emergency Response Teams (CERTs) (on *e.g.* security incidents); *ii*) consumer protection agencies (on *e.g.* online fraud); and *iii*) law enforcement (on other e-crime statistics). Some statistics published by consumer protection agencies, such as statistics on identity theft, are analysed in the privacy section of this report.

National and government computer emergency response teams

Many governments have established and are hosting or co-hosting CERTs that operate at the national level (see Box 4 for a description of the role of CERTs). These *national CERTs* usually have the following roles to play:

1. They act as *in-house CERTs* to the governmental authorities including the regional authorities and municipalities, if a dedicated government CERT does not exist;

2. They act as *CERTs for Critical Information Infrastructures* (CII);

3. They act as *co-ordinator* between all CERTs in the country for operations related to IT security at the national level through *e.g.* information sharing on incidents and vulnerabilities as well as on preventative work.

4. They act as a *point of contact* for similar organisations abroad.

The last point is also true for most large private CERTs. In fact, because of the international nature of cyber-security threats, vulnerabilities and incidents, all CERTs are expected to co-operate among themselves in order to address the risks their constituencies are facing. At an international and regional level, CERTs are collaborating in institutions such as *e.g. i*) the Forum for Incident Response and Security Teams (FIRST); *ii*) TERENA Task Force-Computer Security and Incident Response Teams (European level); and *iii*) Asia Pacific CERT.

Activity reports

CERTs track their service-related activities as listed in Box 4. This can be for billing purposes as in the case of commercial CERTS, for internal reporting as in the case of in-house CERTs, or for informing the public as is the case of national CERTs. Some CERTs publish these statistics in activity reports (usually on a monthly or annual basis), while others publish these statistics through their websites. However, because there is no voluntary commitment or legal obligation to share statistics and data, the level of information sharing varies a lot, ranging from non-existent to daily statistics of main activities.

Box 4. The role of Computer Emergency Response Teams (CERTs)

Computer Emergency Response Teams (CERTs)[1] are IT security expert groups that handle IT security incidents. The first CERT (CERT Coordination Centre, CERT/CC) was created at the Carnegie Mellon University (United States) in November 1988 and funded by the US Defense Advanced Research Projects Agency (DARPA) to respond to the Morris worm that infected computer systems around the world. Since then, more than 250 CERTs have been created worldwide,[2] generally having the following set of services in common:

- **Reactive services:** These services are triggered by a security incident. This includes, but is not limited to, i) issuing alerts and warnings; and ii) handling incidents and vulnerabilities.

- **Proactive services:** These activities aim at improving IT security before an incident occurs. This include, for example, i) provision of technology watch; and ii) security audits; iii) dissemination of best practice; iv) scanning and intrusion detection; v) development of security tools; vi) dissemination of security-related information; and vii) training.

- **Security quality and management services:** These are activities not unique to CERTs intended to leverage and update the knowledge of the constituencies. They include services related to risk analysis, business continuity, disaster recovery, and security consulting.

Although all CERTs may provide these services, they can still have quite a different scope depending on the CERT's origin; that is whether they are hosted and operated by (i) academic or research institutions, (ii) governments, or (iii) the private sector (including non-for-profit CERTs). It should be emphasized that this distinction is often quite arbitrary due to the fluidity of CERTs over the last years. There are several cases of CERTs which started within the academic sector and have been spinned off to also provide commercial for-profit services. For example, academic CERTs such as RUS-CERT of the University of Stuttgart (Germany) mainly provide their services to their hosting academic institution. This is common for all *in-house CERTs*, whose services and activities are directed primarily to serve the need of the organisation where they are located. In-house CERTs are the dominant types of CERTs in the private sector (see Telefonica-CSIRT, Telekom-CERT, Siemens-CERT, CISCO PSIRT).

(1) Sometimes the term Computer Security Incident Response Teams (CSIRTs) is used instead.

(2) See *www.us-cert.gov/aboutus.html*.

Source: OECD

Methodology

However, even if CERTs publish activity-related data, comparing information security threats, vulnerabilities and incidents based on these data remains a challenge for the following reasons:

1. CERTs have to deal with different types of constituencies and different types of incidents, and thus the quantity and quality of activities differ depending on whether academic or research institutions, governments, or the private sector are hosting and operating these CERTs. Thus, statistics from *e.g.* an academic CERT cannot be compared with statistics provided by a national CERT or a CERT of a multinational enterprise without further ado.

2. Because there is no common rule of reporting, CERTs do not report the same categories of data. Some CERTs report only particular incidents, others only alerts and warnings issued, while a minority of CERTs also report the number of security management services provided.

3. Common taxonomies have to be applied by CERTs to assure that data collected are comparable. This is for instance the case for the concept of "incidents", which sometimes includes different security-related events depending on the CERT. Furthermore, subcategories are sometimes difficult to compare because they are aggregated at different levels across CERTs.

Scope and coverage

For this report, the scope will be limited to national and government CERTs. This is because *i*) almost each OECD country as well as accession and enhanced engagement countries have a national and/or a government CERT that can be used as proxy for security-related activities in that country. Furthermore, *ii*) data on national and government CERTs are more likely to be available given their responsibility to inform the public and to be accountable for tax payers' money. Lastly, *iii*) these data are more likely to be comparable, because national and government CERTs share to a large extent the same characteristics. However, national/government CERTs are not always responsible for CIIs. This means that *CERTs with CII responsibilities* can hardly be compared with *CERTs without CII responsibilities*.

So far only data of 14 national/government CERTs have been collected. Table 2 lists the CERTs identified, and shows whether CERTs have CII responsibilities and whether they have published reports and data. Annex Table complements this table by adding the administration supervising the CERT. Data collection has been limited to 14 CERTs for the following reasons: Either *i*) activity reports or data were not available on the CERT's website,[22] or *ii*) activity reports were available, but did not include data related to the CERT's activities[23], or *iii*) the CERT's web site was not accessible.[24] But in most cases, data could not be collected because *iv*) national and government CERTs could not be identified.[25]

Even for CERTs that have published data in their activity reports or on their websites, not all data categories as listed in the next section could be found. It should also be noted that reported activities do not necessarily start with the creation date of the CERTs. As Table 2 shows, the date of creation varies between 1999 and 2011, but in very few cases historical activity reports and data are available on the CERTs' website. In most cases, data are available for 2006 to 2010, with the exception of France, where alerts and notes are available from 2000 to 2010, and Brazil, where incident data are available from January 1999 to August 2011.

Table 2. Government CERTs' responsibilities and report status

Name	Country	Created	Government agencies	CII	Other sectors	Report	Data	Alerts and warnings	Best practice	Incidents
CERT Australia	Australia	Jan-10	✓	✓	✓	✓	✓	✓	✓	✓
GovCERT.AT	Austria	Apr-08	✓	✓		✓	(✓)			✓
CCIRC	Canada	Apr-03	✓	?						
Danish GovCERT	Denmark	Jun-06	✓	?						
CERT Estonia	Estonia	Jan-06	✓	?	?					
CERT-FI	Finland	Jan-02	✓	Telecomm.		✓	✓	✓		✓
CERTA	France	Jan-99	✓	?		✓	✓	✓	✓	
CERT-Bund	Germany	Sep-01	✓	?		✓	✓	✓		
CERT-Hungary	Hungary	Jan-05	✓	✓						
CERTGOVIL	Israel	May-05	✓	?						
NISC	Japan	Aug-03	?	?	?					
KRCERT/CC	Korea	Dec-06	?	?	?	✓	✓	(✓)		✓
GOVCERT.LU	Luxembourg	Jul-11	✓							
CERT-MX	Mexico	Jun-10	✓	✓	✓					
GOVCERT.NL	Netherland	Jun-02	✓	?		✓	✓	✓		✓
Nor-CERT	Norway	Jan-06	✓	✓	✓	✓	✓	(✓)		(✓)
CCN-CERT	Spain	Jan-06	✓	?		✓	✓	✓	✓	✓
CERT-SE	Sweden	May-05	✓	✓	✓	✓	✓	(✓)		(✓)
GovCERT.ch	Switzerland	Apr-08	✓	?	?	✓				
GovCertUK	United Kingdom	Nov-07	✓	?	?					
US-CERT	United States	Sep-03	✓	✓	✓	✓	✓	✓	✓	✓
RU-CERT	Russian Federation	?	?	?	?					
CERT.br	Brazil	Sep-03	✓	✓	✓	✓	✓			✓
CNCERT/CC	China	Oct-00	?	?	✓	✓	✓			✓
CERT-In	India	Jan-04	✓	✓	✓					

Note: (✓) Data exists, (**?**) Data exists but cannot be extracted because of technical reasons.

Data

So far the following data categories have been identified and collected when available:

- **Alerts and warnings issued:** Alerts and warnings are documents intended to prevent an immediate danger. They are usually technical documents about current security threats, vulnerabilities, and exploits, and they provide solutions for mitigating these threats. So far, 10 out of 14 CERTs have published *statistics* on alerts and warnings issued (see Table 2), although most issue alerts and warnings.

- **Best practices and other security-related information published**: They provide an illustration or recent news of some pragmatic measures to implement. This includes in particular opinions outlining vulnerabilities that non-technical home and corporate computer users can take to protect themselves from attacks. So far only three CERTs[26] publish *statistics* on best practices issued (see Table 2), despite the fact that most publish best practices in their reports.

- **Incidents handled:** "Incidents handled" is the most frequent data category reported. However, a commonly agreed definition on what constitutes an incident still does not exist. According to the *Computer Security Incident Handling Guide* of the US National Institute of Standards and Technology (NIST, 2012), an incident is "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices". Further, "an 'imminent threat of violation' refers to a situation in which the organisation has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of a new worm that is rapidly spreading across the Internet". Incidents can be broken down by the following frequently used subcategories:

  - **Malware**: OECD (2009) defines malware as "a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners". This includes, for example, worms and viruses. Based on NIST (2012), for example, US-CERT classifies an incident as "malicious code" if it involves the "*successful* installation of malicious software (*e.g.*, virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application". Almost all CERTs reporting incident numbers also report the number of encountered malware. Some CERTs report malware by using other terms like "malicious code", "worm", or "virus".

  - **Scans/probes/attempted access**: This sub-category includes "any activity that seeks to access or identify a […] computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service".[27] Some CERTs report this incident as "scanning/attack preparation" or "information gathering".[28]

  - **Denial of Service** (DoS) or distributed Denial of Service (DDoS) attacks "seek to render an organisation's website or other network services inaccessible by overwhelming them with an unusually large volume of traffic" (OECD, 2009). US-CERT, for example, classifies an incident as DoS if an attack "*successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS".[29]

  - **Unauthorised access**: This includes the successful intrusion into an information system.[30] "In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource".[31] "Unauthorized

access" includes, for example, the following incidents: "An attacker runs an exploit tool to gain access to a server's password file", or "a perpetrator obtains unauthorized administrator-level access to a system" (NIST, 2012). This category is the most difficult to compare across the CERTs. Although most CERTs use a comparable terminology, some are using sub-categories, which need to be grouped together to make them comparable to the number of unauthorized access. This however is only feasible if all possible means for unauthorised access are reported. [32]

– **Phishing**: Some CERTs also provide statistics on the number of phishing attempts.[33] Some CERTs such as CERT-FI (Finland) uses the term "social engineering", which could be included under phishing as well.

- **Spam**: Some CERTs publishes statistics on spam. Data usually come from the analysis of e-mail filtering systems.

- **Training provided**: CERTs rarely publishes statistics related to the training hours provided to other organisations. So far, only CCN-CERT (Spain) publishes data on training provided on a regular basis.

- **Website access**: CERTs such as CERT.at/GovCERT.AT (Austria) and CCN-CERT (Spain) also publish the number of unique visitors to their web sites.

- **Budget and personnel allocated**: CERTs rarely publish their financial and human resources. When they do, the reported data rather refer to the supervising organisation, *e.g.* in the case of CERT-Bund (Germany), where only data on the budget and personnel of the German Federal Office for Information Security were available.

Potential indicators

Based on these data categories, the following potential indicators listed in Table 3 could be developed, some of which are presented in Box 5. It should be stressed that these indicators are proposed for further discussion, but they would still require common definitions of the categories presented in the previous section.

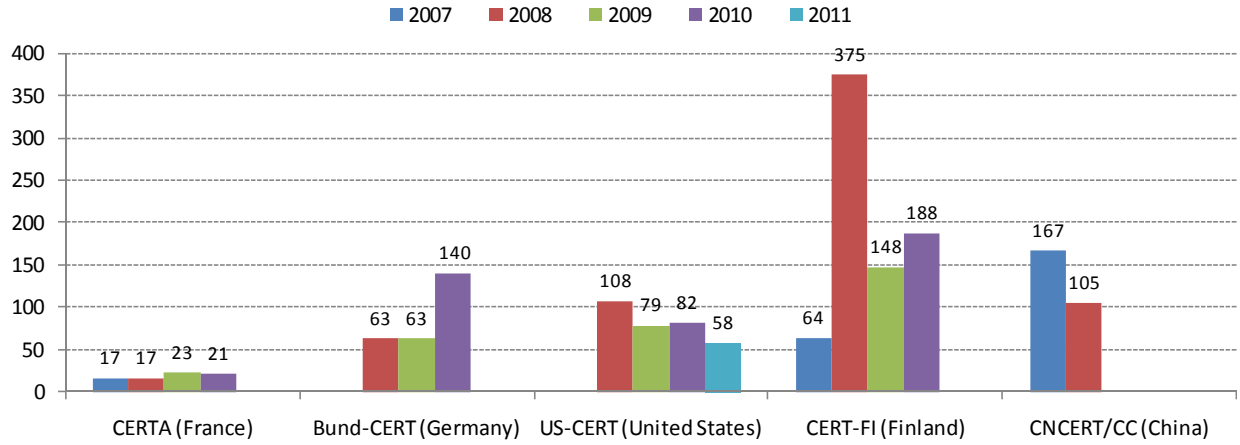
Table 3. Potential indicators from the CERT reports and data

Indicator	Data source	Possible measurement objectives
*** Annual growth in number of alerts and warnings issued by CERT**	Alerts and warnings	Measure prevention as well as ex post threats and vulnerabilities over time.
*** Number of alerts and warnings issued by CERT as share of max. number of alerts and warnings by year**	Alerts and warnings	Measure efficiency of CERTs to prevent exploit. It is assumed that all alerts and warning are relevant to all CERTs' constituencies given the fact that many IT products are used worldwide.
*** Monthly average time lag between discovery of vulnerability and issue of alerts and warnings**	Alerts and warnings	Measure efficiency of CERTs to prevent exploit.
*** Annual growth in number of incidents by CERT**	Incidents	Measure trends in security incidents over time
*** Number of incidents per Internet user** *** Number of incidents per civil servant**	Incidents	Measure incident rates per CERT. Number of Internet users and civil servant is used in the denominator normalize the number of incident. Better denominators may exist such as the total number of servers and desktop PCs of CERTs' constituencies, but are hard to measure.
*** Annual growth in number and share of incidents by CERT and by incident type**	Incidents	Measure trends in specific security incidents, such as malware infection, DoS, scans, etc. over time
*** Number of unauthorized access per number of scans, probes, attempted access**	Incidents	Measure effectiveness of security measures of CERTs' constituencies
*** CERT budget per overall IT government spending**	Budget	Economic measure of the government's priority and awareness of the need to protect and respond to security threats.
*** CERT employees per Internet user** *** CERT employees per civil servant**	Personnel	Human capital resources of the CERT, which can be combined with the number of incidents to show the adequacy of resources to mitigate IT threats and risks.
*** Annual growth in number of training hours provided**	Training	Measure the level of importance of skills for improving IT security.

Box 5. Security indicators based on CERT data

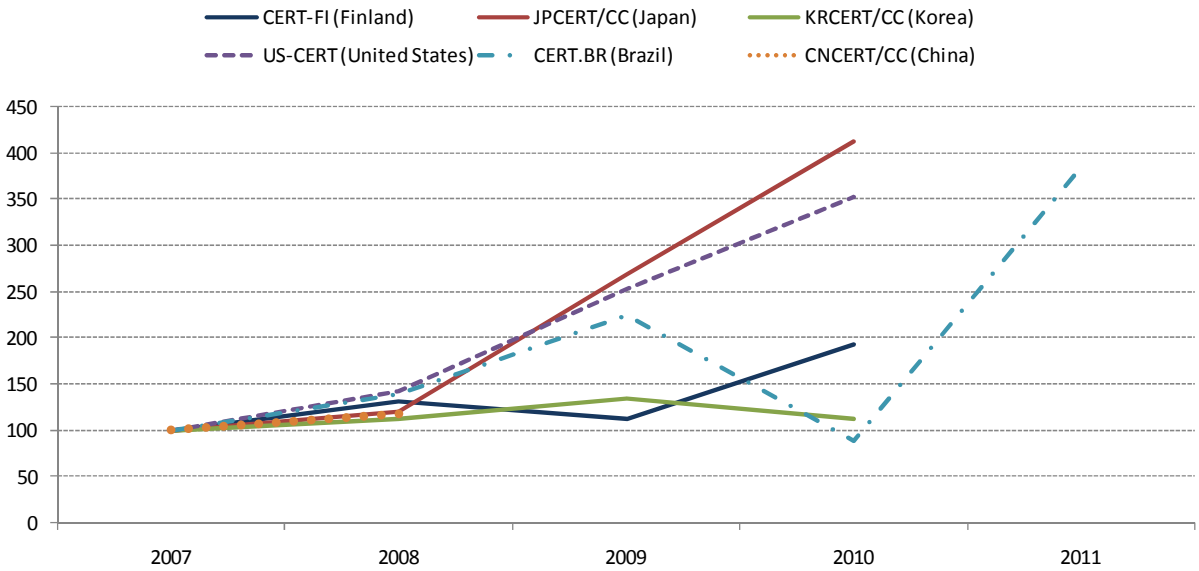
The following indicators are shown as examples to illustrate the potential of data provided by CERTs. Figure 13 shows the number of critical alerts and warnings issued by CERTs in 2007-10. While in some countries such as Finland, France, and Germany, the number of alerts and warnings issued by CERTs has increased over the years, it has decreased in the United States and in China. However, there is still a need to understand the reason for the difference in numbers of alerts and warning. Figure 14, in contrast, shows the trend in the number of incident since 2007. In all countries for which data are available, CERTs have registered a significant increase in the number of incidents compared to 2007. The strongest increase was observed in Japan, the United States and Brazil where the number of incidents has increased almost by a factor of 4 compared to 2007.

Figure 13. Number of critical alerts and warnings issued, 2007-11



Source: OECD based on CERT data.

Figure 14. Trends in the number of incidents, 2007-11
Index, 100 = 2007



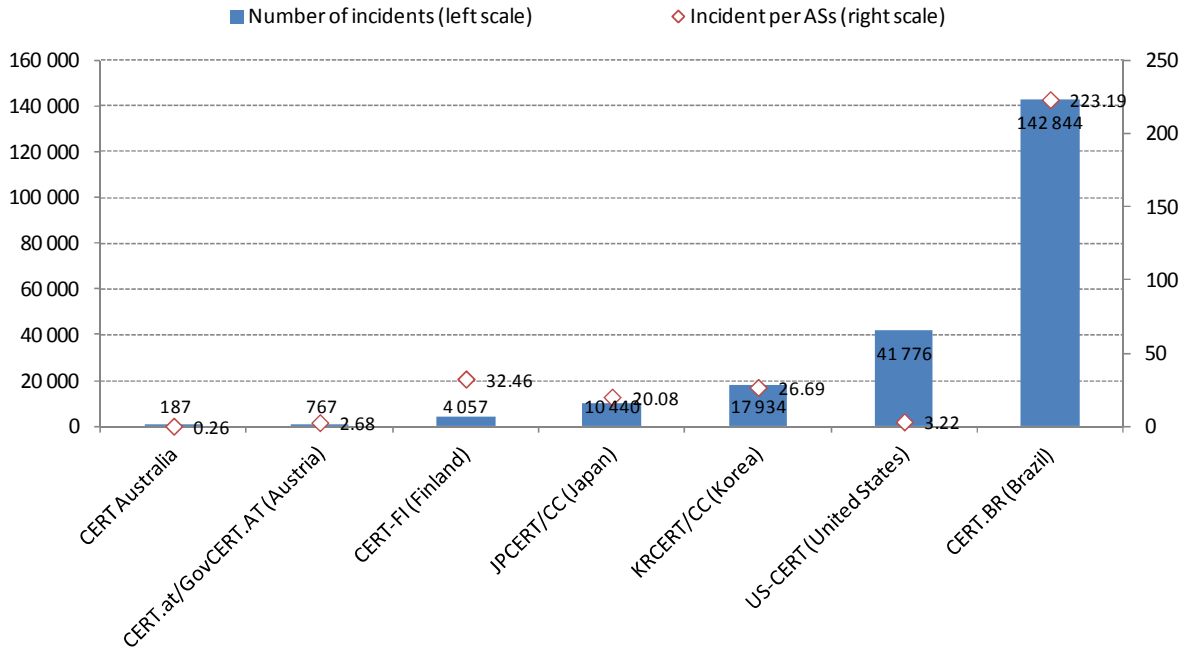
Note: JPCERT/CC (Japan) is a non-government CERT. Incident numbers for CERT.BR (Brazil) in 2011 estimated based on monthly incidents from Jan-11 to Aug-11.

Source: OECD based on CERT data

Box 5. Security indicators based on CERT data (cont.)

Figure 15 shows the number of incidents in 2010, in absolute numbers and per number of routed autonomous systems (ASs). In particular it highlights Brazil as the country with the highest number of incidents per ASs (223 incidents) followed by Finland (32 incidents). However, it should be noted that other statistics could be used as reference, such as the total number of servers and desktop PCs per country, the broadband penetration rate, or the number of Internet-connected firms. Figure 16, finally, highlights the types of incidents as the share of the total number of incidents in 2010. It shows, for example, that malware and phishing attacks remain the biggest threats CERTs are facing, followed by unauthorized access (failed and success attempts).

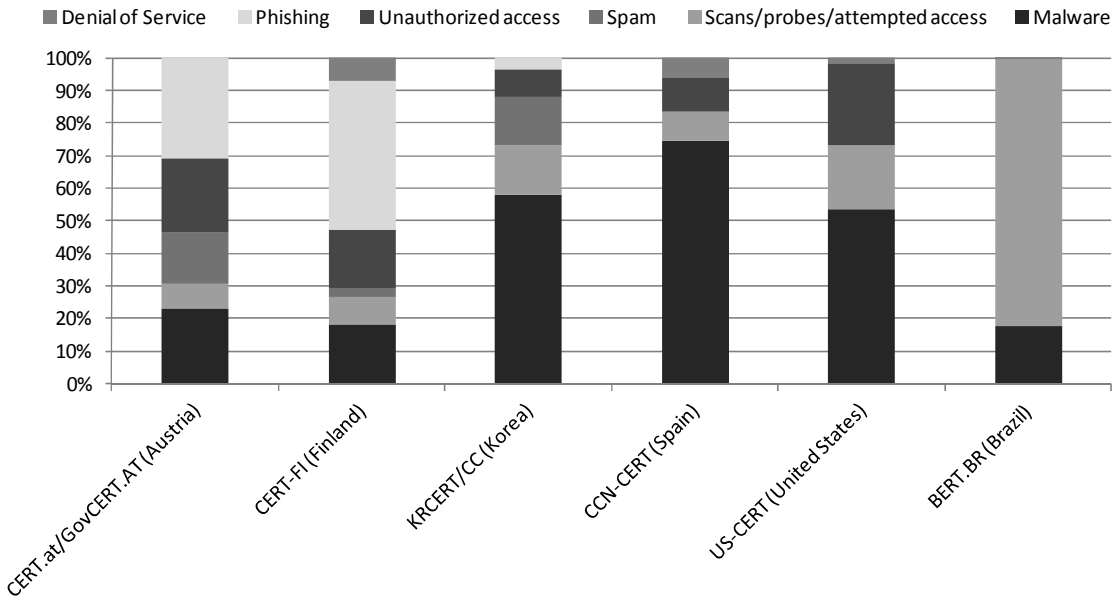
Figure 15. Total number of incidents reported by CERTs, 2010



Source: OECD based on CERT data.

Figure 16. Type of incident as share of total number of incidents by CERT, 2010

Percentage



Source: OECD based on CERT data.

Internet based statistics and surveys

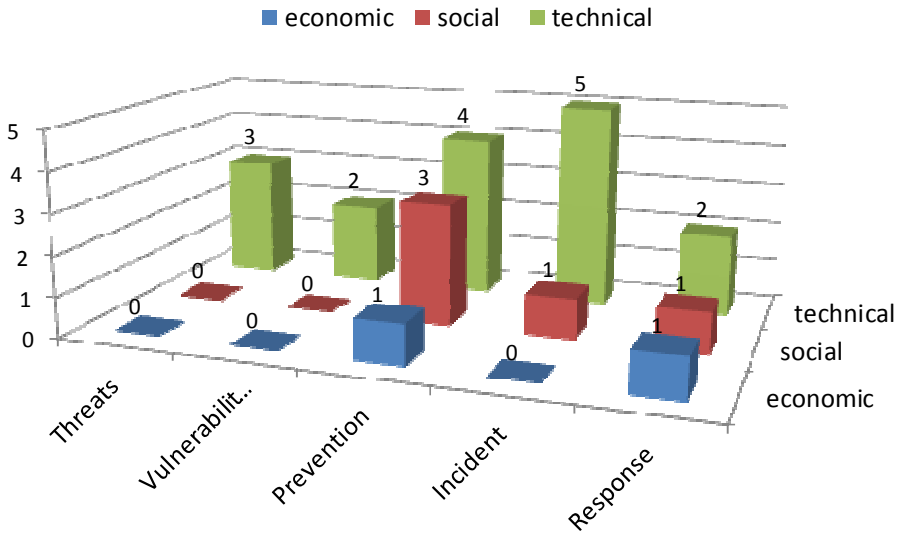
Besides the data listed in the previous section, some CERTs also collect additional data, which are unique and thus cannot be compared across CERTs. In most cases, these very interesting data sets are collected directly from Internet traffic by using, for example, a *honey net*. CERT-SE (Sweden), for example, operates a honey net and publishes daily statistics about attacks of the last eight days on the web. Unfortunately, historical data do not seem to be available. CERT-Bund (Germany), as another example, collects data on intercepted or stolen personal data, that malware have transferred to *drop zones*, which are "servers controlled by the perpetrators […] deployed for identity fraud purposes" (Federal Office for Information Security, 2011).[34] Data of more than 200 drop zones were collected and analysed, and indicators based on these data are available in the annual report of the German Federal Office for Information Security (see Federal Office for Information Security, 2011).

Some CERTs have, in addition, collected data through surveys. AusCERT (former national CERT in Australia), for example, partnered with the Australian High Tech Crime Centre (AHTCC), the Australian Federal Police (AFP) and state police departments to undertake the Australian Computer Crime and Security Surveys.[35] The survey was done on a yearly basis starting in 2002, but was discontinued in 2006-2007. INTECO-CERT, which in conjunction with CCN-CERT and IRIS-CERT forms the Spanish national CERT structure, is also conducting information security and e-trust related surveys in Spain. What is interesting here, is that INTECO-CERT combines household data with Internet-based data of an identical sample of more than 3 500 users, in order to compare users' perception of computer security with the real situation. These users have been provided with a specifically designed software that examines security incidents in home computers. At the same time the perception and trust level of these households are assessed by means of online surveys carried out every four months.[36]

Gap analysis

As in previous sections, potential indicators presented in Table 3 are systematically mapped into the analytical framework (see Figure 17). The concentration of technical indicators, in particular in the area of prevention and incidents, as well as in that of response, threats and vulnerability can be observed. This is no surprise given the mission of CERTs, which is primarily to receive, review, and respond to security incidents and IT vulnerabilities and to provide technical assistance where such need is required. However, what is striking is the relatively low share of technical indicators in the area of response, given that it is the role of CERTs to respond to security incidents. Indicators on, for example, the reaction time between the identification of an incident and the first action of the CERT could provide additional insights on the efficiency of CERTs' operations. Other examples may include indicators on the costs and time of the analysis of an incidents and the application of first remedies.

Figure 17. Number of security indicators based on CERT data by type



Source: OECD based on CERT data.

Law enforcement agencies

Some law enforcement agencies (LEAs) collect data on Internet-related crimes. In some cases, data are generated from legal proceedings. In Germany, for example, statistics are available on ICT-related crimes that are specified under the German Penal Code (see OECD, 2005b). This included: (Art. 202a) spying on data, (Art 263a) computer fraud, (Art. 269) falsification of evidence documents, (Art. 303a) alteration of data and (Art 303b) computer sabotage. According to this data, 98% of all ICT-related crime is related to computer fraud, pursuant to Article 263a of the German Penal Code. The number has increased from 1 561 in 1995 to 2 670 in 2002. This is an average increase of 8% yearly.

However, data on e-crime are dispersed across different sources of statistics leading to different definitions of what for example constitutes a cybercrime being one of the major issues. The Council of Europe (CoE) convention on cybercrime could be used to develop common definitions. However, some efforts would still be required in order to have comparable statistics across OECD economies on e-crime.

Consumer protection agencies

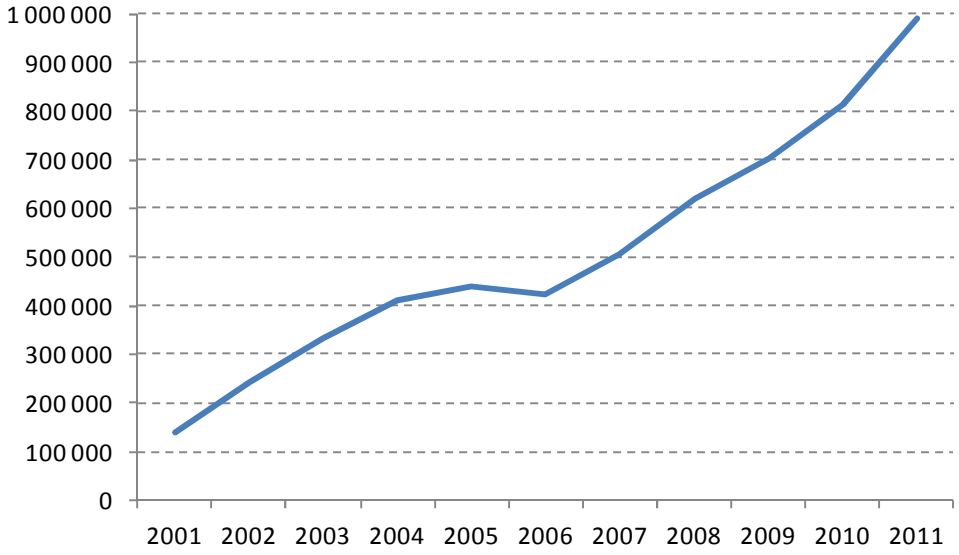
Some consumer protection agencies have a mandate to address privacy- and security-related issues, and have collected data on consumer issues that are relevant to measure security, privacy and trust online. Data of interest for this report include in particular data on *online fraud* and *identity theft*. The latter is, however, presented within the privacy section of this report. In the following paragraphs, data collected by the Consumer Sentinel Network (CSN) are presented to illustrate the potential of this type of data sets.

The CSN database is an online database which was created in 1997 by the United States Federal Trade Commission (FTC) to collect complaints on fraud and identity theft reported by consumers. The complaints stored in the database are those filed with the FTC, as well as a number of other bodies[37], and are made available to law enforcement agencies which are members of the network. Today, the CSN complaints relate to areas as diverse as: "Identity Theft; Do-Not-Call Registry violations; Computers, the Internet, and Online Auctions; Telemarketing Scams; Advance-fee Loans and Credit Scams; Sweepstakes; Lotteries; and Prizes; Business Opportunities and Work-at-Home Schemes; Health and Weight Loss Products; Debt Collection; Credit Reports; and Financial Matters".[38] Box 6 present the number of complaints related to online fraud in the Consumer Sentinel Database.

Box 6. Indicators on online fraud in the Consumer Sentinel Database

Each year, the FTC publishes the Consumer Sentinel Network (CSN) Data Book. It makes available to the general public detailed statistics about the complaints received, which currently amount to more than 6.1 million entries.[39] The figures are updated every year, to account for the different reporting times of the contributors. Figure 18 shows the number of complaints related to *online fraud* in the Consumer Sentinel Database. Between 2000 and 2011, the number of complaints related to online fraud has increased by almost 25% yearly, a rise that is undoubtedly related to the expanding use of the Internet and therefore needs to be assessed further through additional data. In particular, complaints in CSN are self-reported and unverified, and they do not necessarily represent a random sample of consumer injury for any particular market. For these reasons, year-to-year changes in the number of fraud and/or identity theft complaints do not necessarily indicate an increase or decrease in actual or perceived fraud and/or identity theft in the marketplace.

Figure 18. Number of complaints related to online fraud in the Consumer Sentinel Database, 2001-11



Source: OECD based *on* U.S. FTC, Consumer Sentinel Network Databook January-December 2011 (Feb. 2012)..

Private organisations and data sources

Private organisations, including commercial as well as not-for-profit organisations, are important allies in the development of better indicators for policy making. This is even more the case in the area of Information security, where the largest data sets are generated, collected and analysed by security expert groups including, among others, IT companies and the scientific community. Key groups include: *i*) security tool providers; *ii*) software vulnerability databases; *iii*) network services and equipment providers; *iv*) certificate authorities; *v*) honey net operators; and *vi*) consulting companies. These groups are dealt with in the section below. Other sources could be included, as shown by some anecdotal evidence presented in Box 7.

Box 7. Some anecdotal evidence related to security

Anecdotal evidence is the weakest form of evidence for policy making. However, it can be useful in areas where other evidence does not exist or is not available in the short-term. In this case, anecdotes should be collected and evaluated systematically to assure a certain degree of representativeness. Examples include:

1. Statistics based on leaked passwords of internet accounts suggests that most users still use weak passwords to protect their online profiles. A significant amount of users (around 25%) uses their first name as their password. Another frequently type of used passwords consists of a sequence of identical characters such as "111111". In other frequent cases a series such as "123456" and so on is used as passwords. More than one third of all passwords were words available in dictionaries, the most frequent being "password". What is most striking is that around 90% of all users used the same password across different services (Hunt, 2011).

2. The cost for renting a bot net is decreasing. Renting a DDoS botnet can cost around USD 200 per 10 000 bots per day (USD 0.02 a bot). A recent example is the TDSS botnet. As one of the most sophisticated botnets today according to security firm Kaspersky Lab, it is advertised to have more than 24 000 bots. Services such as web proxy services are provided for USD 25 per month to consumers; this is almost 10 bots per cent (Krebs, 2011).

3. Demand and salaries for IT security professionals continue to increase. According to IT training provider GlobalKnowledge (2010), IT security skills ranked second among the top 10 IT skills in 2010. Furthermore, demand for IT security professionals in the United Kingdom increased in 2011, mainly driven by high-profile cyber attacks and growing spending on cloud computing security, increased use of penetration testing services, and "the January 2012 deadline for all PCI DSS assessments to be under version 2.0 of the standard" (Ashford, 2011). As a result, salaries of IT security professionals changing employers peaked at 13% in the first half of 2011.

Security tool providers

Providers of security software such as Symantec, Kaspersky, McAfee,[40] PandaLabs, and more recently Microsoft are in a very good position to collect data on security threats. In order to continuously improve the ability of their software to detect malware, these firms are collecting data on active malware. This is done through different mechanisms, all having in common the fact that they are based on the Internet as the main source and distributer of data. For example, Symantec, through its Global Intelligence Network, has "more than 240 000 sensors in more than 200 countries and territories" to monitor attack activities (Symantec, 2010). Microsoft, through its *Internet Explorer* and its search engine *Bing* is collecting data on phishing sites, besides the data on malware it collects through its security tools. All these data are regularly published in reports such as the *Symantec (2010) Internet Security Reports*, the *McAfee (2011) Threats Reports*, the *MessageLabs Intelligence (2010) Reports* and the *Microsoft Security Intelligence Report* (2011) (see Box 8).

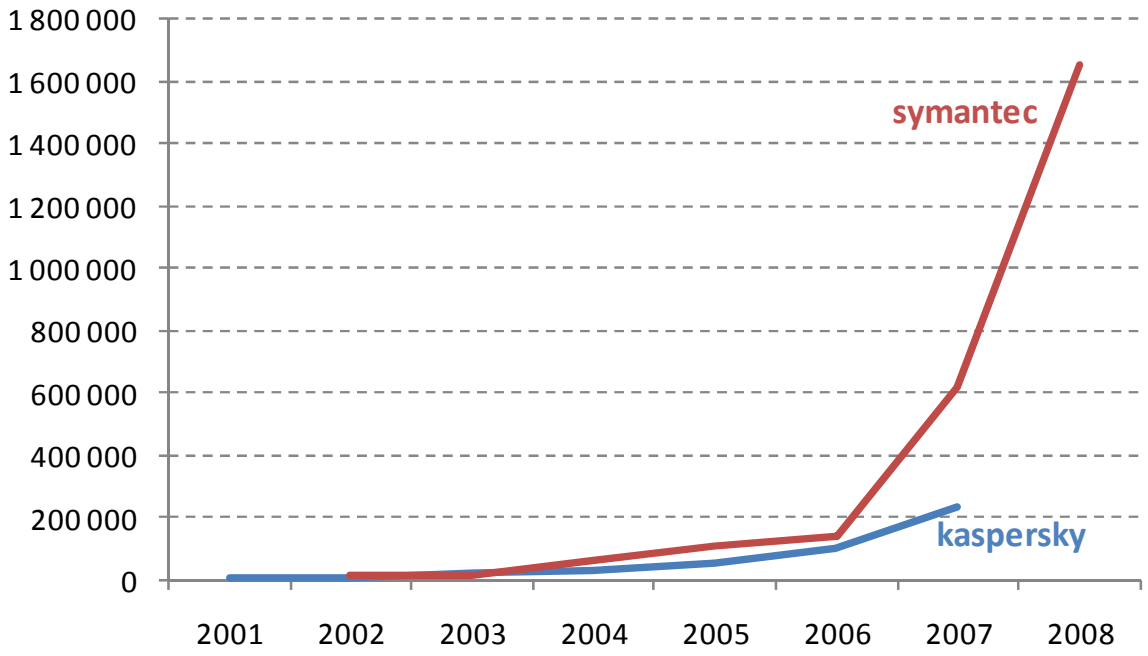
It should be noted, however, that comparing these numbers across different data sets and data providers is challenging because of missing standards in the way variants are being taken into account. Some firms may include minor variants of the same malware type in which case the numbers would obviously be much higher than if only major or no variants would be included. Furthermore, variants have become even more difficult to identify due to the increasing use of *polymorphism* in the malware development process.[41] As a result, the number of variants is only limited by the degree of sophistication of the malware, and thus counting variants becomes less meaningful if interpreted in its traditional sense. However, the number of discovered variants can be reinterpreted as an indicator for the level of sophistication of the malware, making this statistic still useful for assessing the level of threat originating from the malware.

Box 8. Malware statistics

A first set of indicators measuring the magnitude of information security threats are statistics on discovered malware. Available figures on the number of malware suggest that new malware and their modifications (*i.e.* variants) are being developed at exponential rates. Figure 19, for instance, shows the number of new malware as detected worldwide by IT security company Symantec (based in the United States) and Kaspersky (based in the Russian Federation).

According to this figure, the number of newly created malware is doubling or even tripling each year. Another indicator confirming the increase in new malware is the size of antimalware signature files. According to Microsoft (2011), the size of today's antimalware signature files has increased from less than 1 (MB) in 2002 to more than 100 MB in 2011, an compound annual growth rate (CAGR) of 67% per year.

Figure 19. Number of new detected malware worldwide, 2001-08

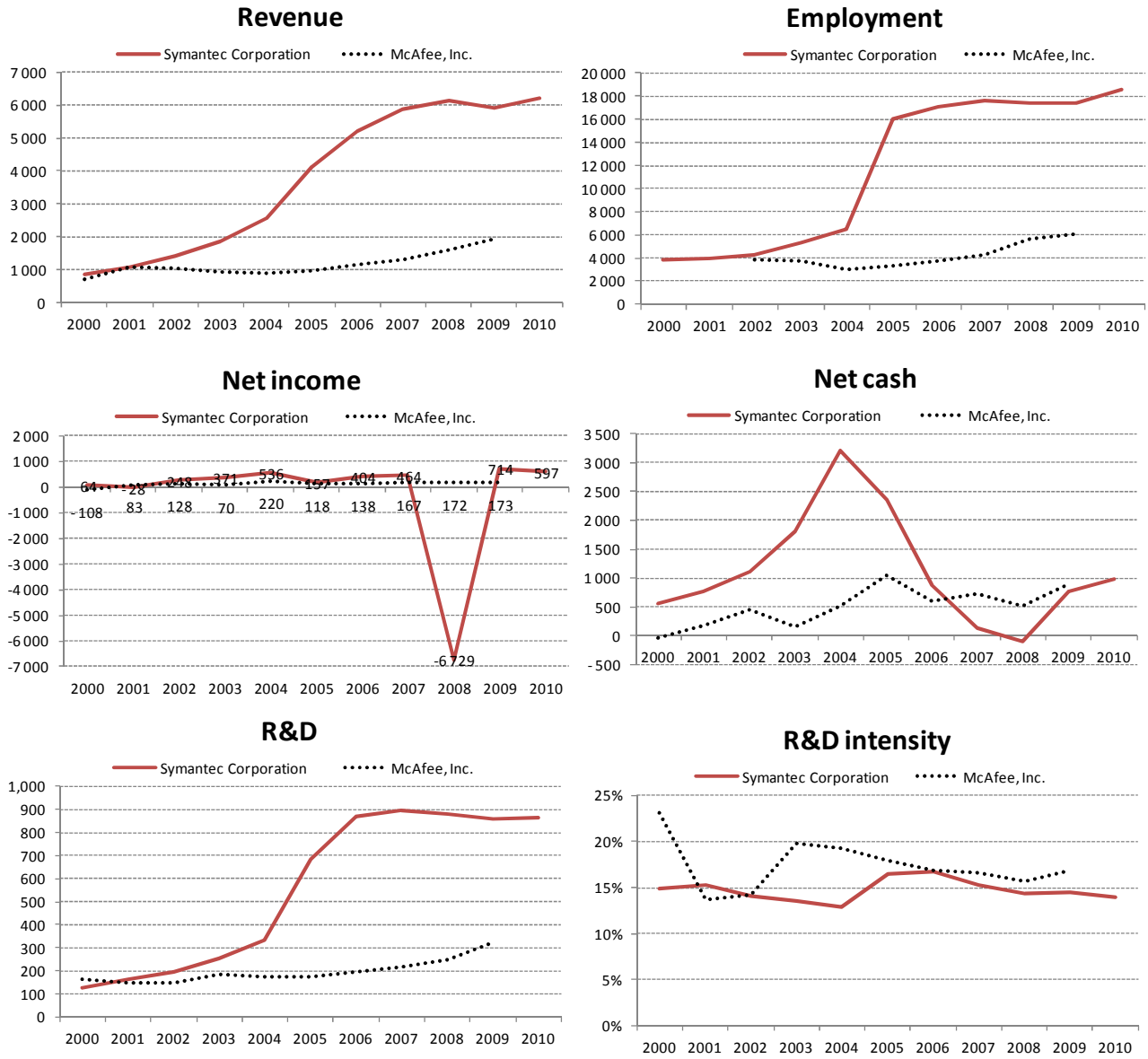


Source: OECD based on data from Symantec Corporation: Internet Security Threat Reports.

Box 8. Security indicators based on IT security companies' reports

Figure 20 shows some key financial indicators for Symantec Corp. and McAfee, Inc.[1] One key indicator that may need some explanation is research and development (R&D) intensity. It is basically defined as R&D expenditure as a share of sales revenue. Symantec and McAfee invest on average around 15% of their revenue on R&D. They are thus more R&D intensive than the average top 250 ICT firms, which spent around 6% of revenue on R&D during 2009 (see OECD, 2010c). This suggests that IT security is significantly R&D intensive and that innovation is thus key to promote a secure Internet economy. Further analysis on patent activities in this field could be done to verify this hypothesis.

Figure 20. Financial indicators for Symantec Corp. and McAfee, Inc. , 2000-10
USD millions and R&D intensity in percentage



(1): McAfee has been acquired by Intel Corp. for USD 7.68 billion in 2010.

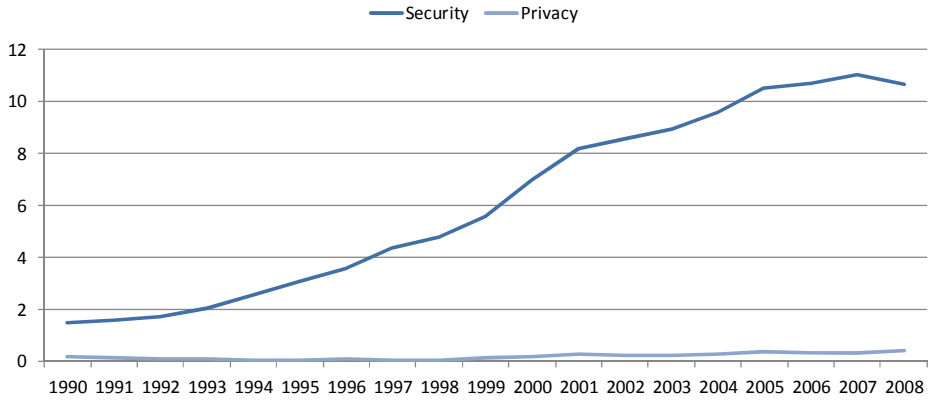
Source: OECD Information Technology Database, compiled from annual reports, SEC filings and market financials

Box 8. Security indicators based on patent and trademark data

Figure 21 shows that the number of PCT patent applications related to information security and privacy is increasing faster than the number of ICT patent applications. In 2008, for each 1 000 ICT patent application there were around 11 patent applications related to information security. This share has increased by a factor of 2 to 3 in 2008 compared to 1998. However, since 2007 the share of ICT patent applications related to security has stagnated or even decreased. This indicates that the number of security-related patents is growing at a slower pace compared to overall ICT patent applications. Further analysis reveals that most patent applications related to security have been filled by organisations in the United States, followed by organisations in China, Germany, France, and United Kingdom. Trademarks are another promising alternative to patent statistics for measuring innovation in security (and privacy). As Figure 22 presents, the number of trademark applications in security and privacy per thousand ICT trademark applications in the United States Patent and Trademark Office (USPTO) are around six times higher than for patent applications. In 2010, around 50 trademarks per thousand ICT trademark related to security have been registered in the USPTO. In particular, one can note that trends observed in the USPTO confirms patterns observed in patent applications.

Figure 21. Relative number of patent applications in information security[1] and privacy[2] filled under PCT, 1990-2008

Per thousand ICT patent applications

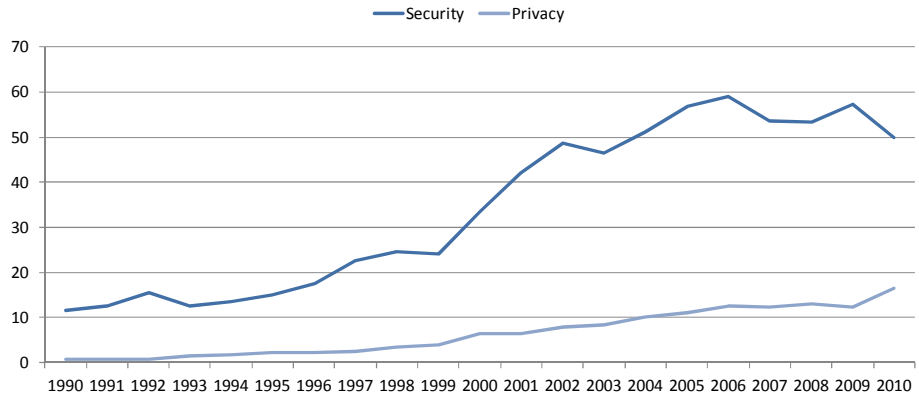


(1) Security-related applications are identified with keywords such as "recovery" "virus", "spyware", ("security" and "computer")
(2) Privacy-related applications are identified with keywords such as "anonymity", "identity", "privacy".

Source: OECD, Patent Database.

Figure 22. Relative number of trademark applications in information security[1] and privacy[2] at USPTO, 1990-2010

Per thousand ICT trademark applications



(1) Security-related applications in classes 9, 38, 42, 45 with keywords "Recovery" "virus", "spyware", ("security" and "computer")
(2) Privacy-related applications in classes 9, 38, 42, 45 with keywords "anonymity", "identity", "privacy".

Source: OECD, based on data of the US Patent and Trademark Office (USPTO).

Honey net operators

The use of honey nets as a source for security related statistics has already been discussed in the section on CERTs. To recall what honey nets are: A *honey net* is a network of *honey pots*. And a *honey pot* is a system that emulates a set of vulnerable IT services. It is usually "isolated, protected and guarded, but gives the appearance that it contains a vulnerable system of value to the attacker".[42] It thus acts as fly-paper for malicious code and gives security experts the possibility to analyse attacks and malicious code used in real-time or *ex post*. Besides CERTs such CERT-SE (Sweden), a growing number of security expert groups (including IT security companies) rely on honey nets to collect data on current IT threats. This especially includes data on botnets, that are "groups of malware infected computers also called 'zombies' or bots that can be used remotely to carry out attacks against other computer systems" (OECD and APEC, 2009; see Box 9).

One of the major advantages of using *honey net* data is that as they are Internet based, big data on security threats can be collected and made available to researchers around the world automatically and in real-time.[43] Furthermore, data sets can be linked to other pertinent data sets in order to gain additional insights.[44] Another advantage specific to combating bot nets is that in most cases data on IP-addresses of the machines participating in attacks can be recorded, enabling researchers to analyse bot net attacks by country and ISPs (see van Eeten *et al*, 2011). Furthermore, honey net data are "not limited to machines in a single botnet, but can identify machines across a wide range of botnets that all participate in the same behaviour, such as the distribution of spam" (van Eeten *et al*., 2010). This improves the representative slice of the problem. However, due to possible false positives, it also decreases the accuracy of the measurement.[45]

Network services and equipment providers

Some network services providers such as Akamai and network equipment vendors such as Cisco Systems are collecting data on Internet-related traffic in order to better understand traffic patterns and to optimize the use of their network equipment. This also includes identifying, collecting and analysing malicious traffic data. Akamai, for example, "uses its globally distributed content distribution network to gather data on the state of the Internet, including data on attack traffic or Denial of Service (DoS) attacks, hacking attempts and DNS hijackings […] originating from 200 unique countries" (OECD, 2011e). These data rely on similar techniques as presented above. Examples for indicators based on Akamai data are presented in Box 10.

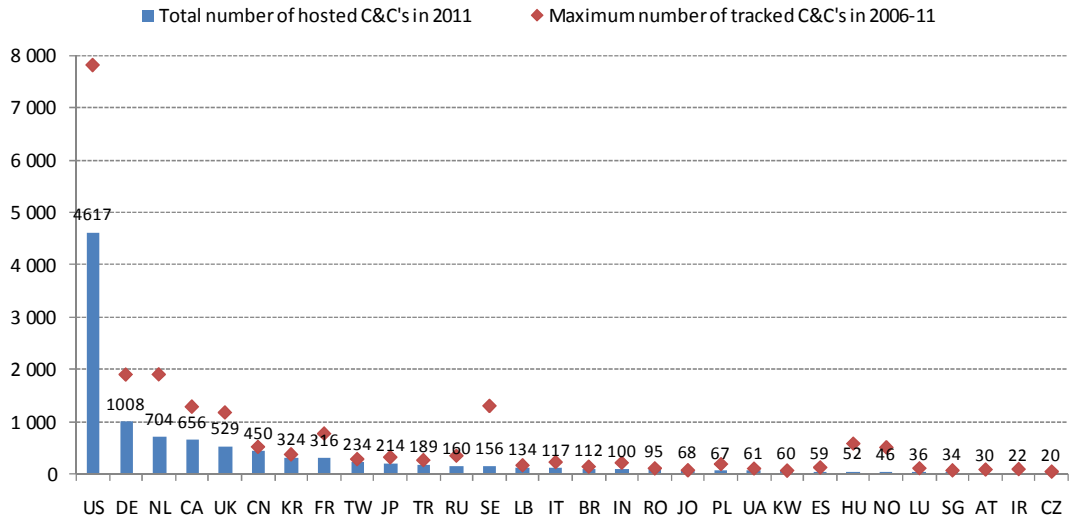
Vulnerability databases

Software companies are regularly issuing patches to respond to discovered vulnerabilities in their products. These vulnerabilities have been collected by different bodies and made available in databases. One prominent example is the National Vulnerability Database (NVD) which is also being used by CERTs such as US-CERT (United States). It is "the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP)". It provides vulnerability data by *i*) vulnerability categories; *ii*) severity (base score range); *iii*) access vector; *iv*) access complexity; *v*) authentication; *vi*) confidentiality; *vii*) integrity; and *viii*) availability. Another example includes the Open Source Vulnerability Database (OSVDB) which is an independent and open source database created to provide "accurate, detailed, current and unbiased technical information on security vulnerabilities".[46] OSVDB includes data on vulnerabilities since 1965 (see Box 11).

Box 9. Measuring botnet-related threats

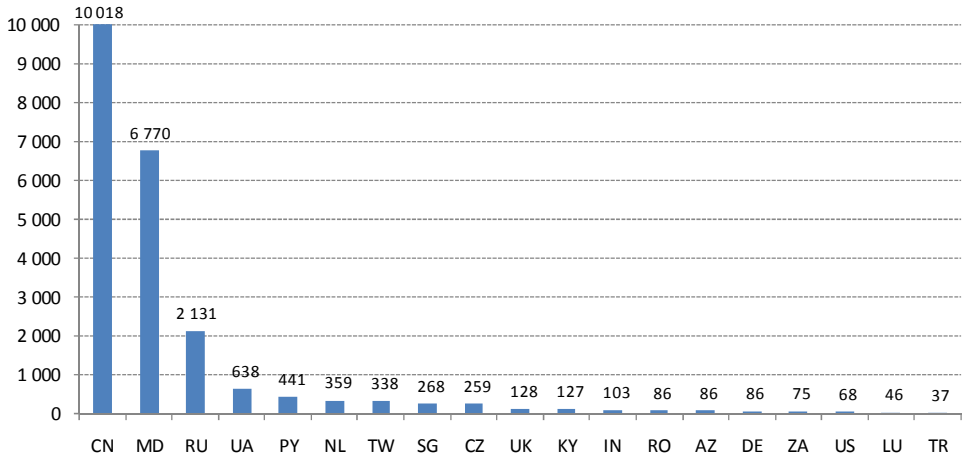
Statistics on botnet's activities are typically collected in real-time via the Internet itself. For example, the Shadowserver Foundation, a "volunteer watchdog group of security professionals" is collecting botnet-related data among others. According to these data the total number of bot- and C&C machines is decreasing slowly since 2009-2010, in particular in countries such as in the United States, the Netherlands, Sweden, Germany, and the United Kingdom to cite a few (see Figure 23). Despite the decrease, however, botnets still remain very active with the five most active C&C's having IP addresses located in China, Moldova, Russia, Ukraine, and Paraguay (see Figure 24). A single C&C server in China, for example, initiated on average more than 10 000 DDoS attacks between 2006 and 2011. That is on average more than 1 600 DDoS attacks per year.

Figure 23. Number of unique C&C machines by economy, 2006-11
Top 30 countries



Source: OECD based on data from the Shaow Server Foundation

Figure 24. Average number of DDoS attacks initiated by a single C&C machine by country, 2006-11
Top 30 countries



Source: OECD based on data from the Shadow Server Foundation.

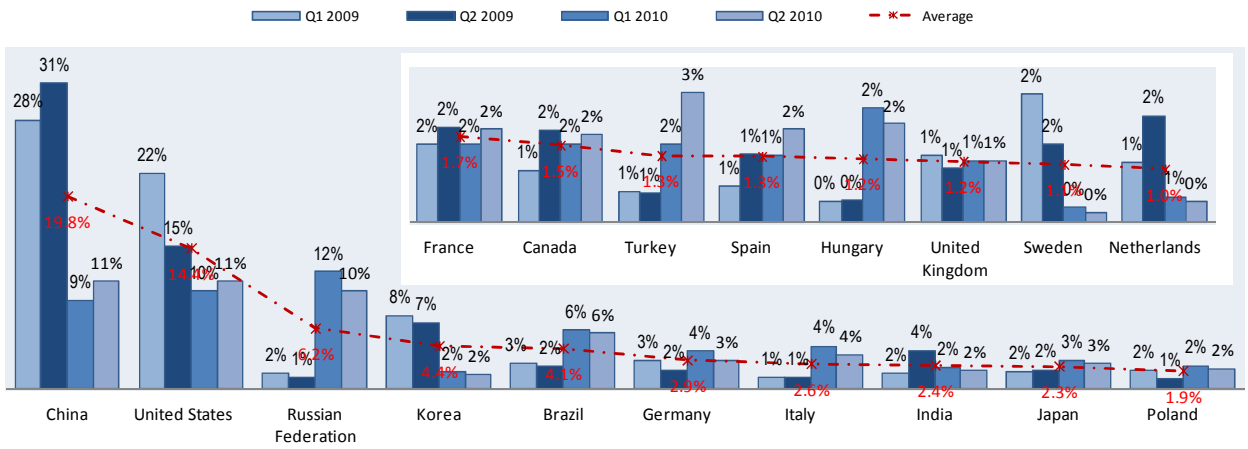
Box 10. Security indicators on attack traffic based on Akamai

Akamai collects real-time data on captured "packets generally issued from automated scanning Trojans and worms that seek to infect new computers by scanning randomly generated IP addresses" (OECD, 2011d). Data collected include (*i*) number of connections, (*ii*) source IP address and port, and (*iii*) destination IP address and port. **Error! Reference source not found.** present the share of attack traffic by country of origin. Since a greater level of Internet usage may lead to higher levels of attack traffic, the level of Internet usage needs to be taken into account. This can be done by taking the number of routed autonomous systems (ASs) into account. As Figure 26 then shows, the high magnitude of attacks in *e.g.* the United States can partly be explained by the high number of ASs.

Finally, one should highlight the following two points when interpreting the data collected by Akamai: First, the country in which attack traffic originates does not necessarily indicate where the attack was launched, but instead represents the location to which the attack was allocated. Second, the data are based on traffic observed by Akamai, and do not represent the entire Internet (see OECD, 2011d).

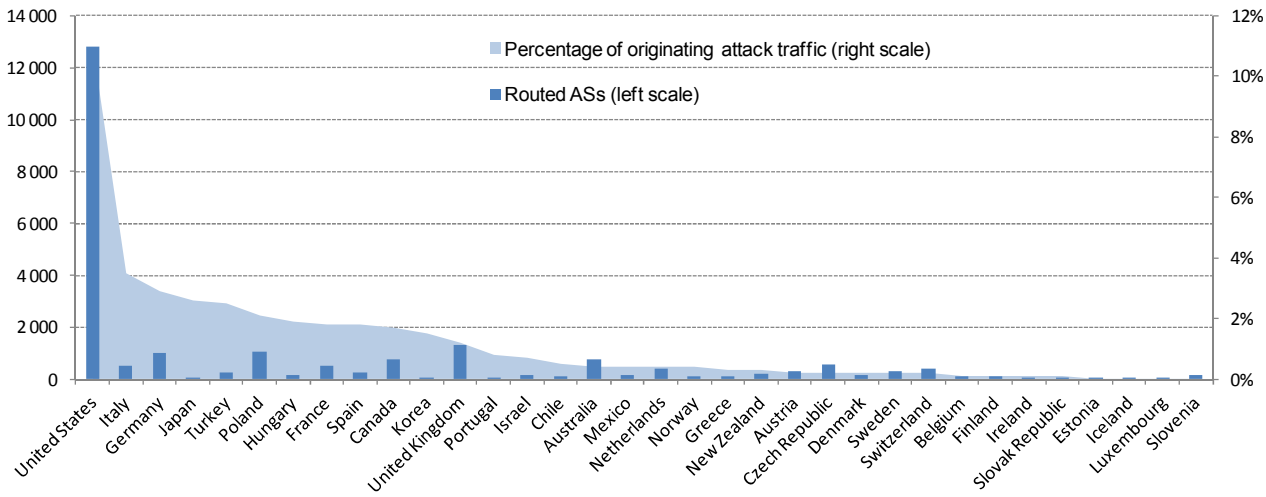
Figure 25. Attack traffic, top originating countries, 2009-10 (mid-year)

Percentage of traffic



Source: OECD (2011d) based on Akamai, 2010, The State of the Internet (*www.akamai.com).*

Figure 26. Originating attack traffic and routed ASs in OECD countries, year-end 2010

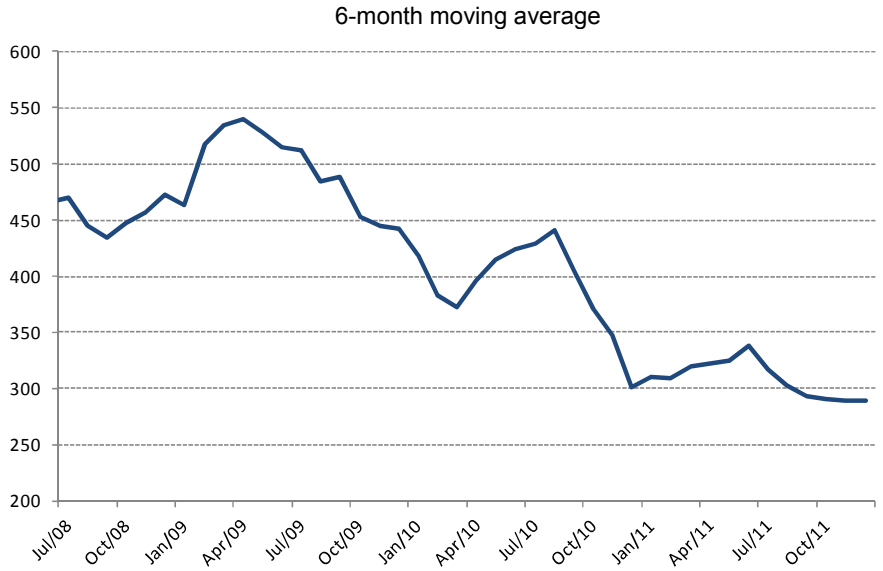


Source: OECD (2011d) based on Akamai, 2010, The State of the Internet (*www.akamai.com).*

Box 11. Security indicators based on IT vulnerability databases

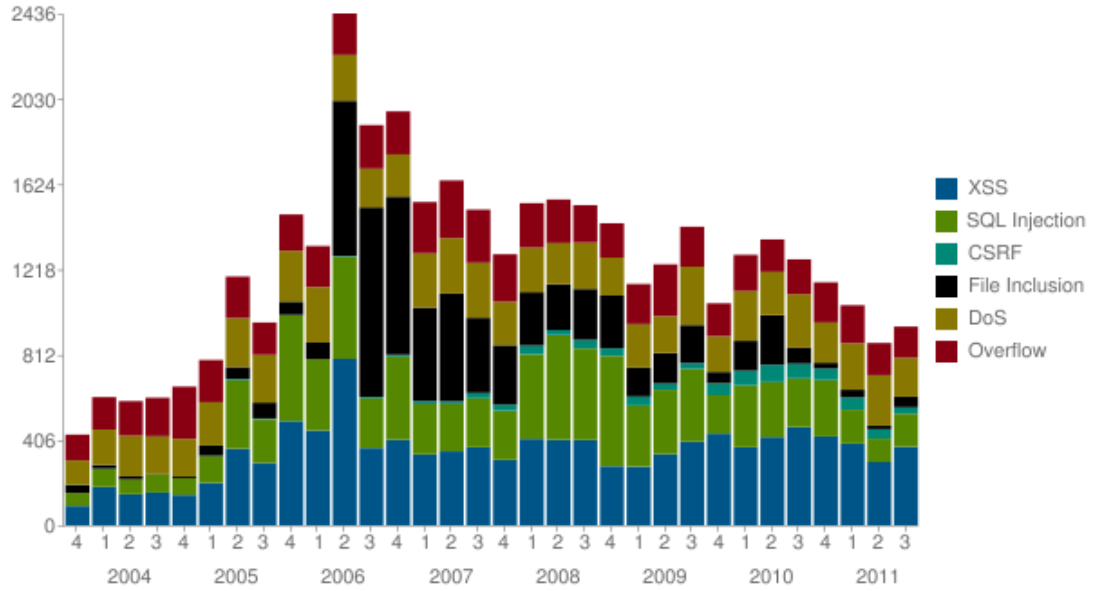
Figure 27 shows the number of newly detected vulnerabilities in NVD published by US-CERT. The number has been decreasing since 2008. However, as is the case for many statistics presented in this report, this numbers have to be interpreted carefully when used out of context. In this case, the decrease in the number of vulnerabilities could be due to *i*) an overall improvement in the quality of software; *ii*) a decreasing ability of security experts to discover additional vulnerabilities; or *iii*) an increasing unwillingness to publish IT vulnerabilities to the public. Figure 28 shows that, although the overall number of vulnerabilities discovered is decreasing overall, some types of vulnerabilities are increasing, namely those exploitable through Denial of Service (DoS) and cross-site scripting (XSS), both being web application specific.

Figure 27. Monthly number of vulnerabilities in NVD as published by US-CERT, July 2008-November 2011



Source: OECD based on US-CERT reports

Figure 28. Quarterly number of vulnerabilities in OSVDB by type



Source: OSVDB

Certificate authorities

A certificate authority (CA) is "a third party organisation which is used to confirm the relationship between a party to the *https* transaction and that party's public key. Certification authorities may be widely known and trusted institutions for Internet based transactions".[47] They can be publicly owned and/or operated by governments or private and commercial. Commercial CAs in particular gain their revenues by selling "certificates with different prices and features, offering different levels of assurance (*e.g.* low assurance certificates, high assurance certificates, extended validation certificates, etc.)" (OECD, 2011d). Furthermore, most commercial CAs offer "warranty for the users of an SSL certificated site, which will compensate the end user if the site turns out to be fraudulent" (OECD, 2011d).

Unfortunately, CAs very rarely publish statistics on *e.g.* the number of certificates issued and the total revenue gained through the provision of certificates (the exceptions are some government agencies such as the German Federal Office for Information Security). These statistics, however, would be very useful for analysing trends in the deployment of secure servers and the market of SSL certificates. This is even more the case in the light of current series of cyber attacks against CAs such as DigiNotar, where a better understanding of the market dynamics and the underlying incentives would be needed to better assess the impact of incidents. So far, surveys done by companies such as Netcraft remain one of the rare sources for data on SSL certificates usage (see Box 12).[48]

IT consulting, audit and related companies

IT consulting, audit and other related companies are the last group of private organisations that are considered in this work. Some of these firms such as PricewaterhouseCoopers (PwC), Deloitte Touche Tohmatsu Limited (Deloitte), KPMG, and the Computer Security Institute (CSI) are collecting security-related data, mainly through surveys of IT security experts and IT executives. These data sets can be interesting for the development of economic indicators, given that they often include questions related to *e.g.* the costs of security breaches and the level of investment in IT security. However, as highlighted in the introduction of this report, surveys assume that the answers provided by respondents are correct, which cannot always be assumed in the area of security, in particular if a transparent and well-defined methodology is missing, and the sample size and response rate are too low.

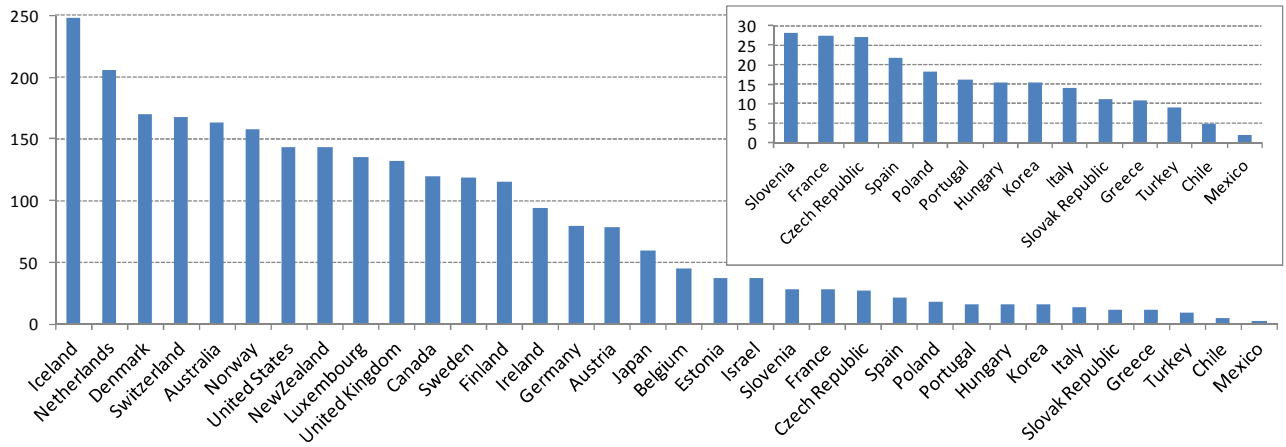
For example, the CSI *Computer Crime & Security Survey* conducted surveys since 1999. In 2008, for example, it surveyed 522 computer security practitioners in US corporations, government agencies, financial institutions, medical institutions and universities (see Box 13; CSI, 2008). However, the number of respondents sharing details on their financial losses was continuously decreasing. While only 144 of 522 (28%) respondents answered questions about financial losses in 2008, this was 40% in 2007 and almost 50% in 2006. This suggests that the data collected by CSI could be biased towards lower losses in the later years. It is interesting to note that CSI (2010) did not publish the most recent figures on financial losses in their 2010 survey report because the sample of firms was too small: only 77 (21%) of the 351 surveyed organisations reported their financial losses.

A number of private organisations are also collecting statistics on IT security related skills. This includes in particular certification bodies issuing certifications for security-related skills to professionals. The International Information Systems Security Certification Consortium $(ISC)^2$, for example, provides certifications for security-related skills in more than 130 countries (see Box 14).

Box 12. Security indicators on SSL certificates and secure servers based on Netcraft

Figure 29 shows the number of secure servers per 100 000 inhabitants. As highlighted in the previous section, a better indicator could be derived by counting the number of secure servers per total number of servers. Still, this figure is best interpreted in conjunction with the data extracted from the OECD model surveys, namely the share of businesses using a secure protocol for the reception of orders via Internet in 2008. Figure 30. 0 shows the market share of certificate authorities. It highlights in particular that VeriSign, Go Daddy, and Comodo together account for more than 85% of the total market of certificates (in number of certificates).

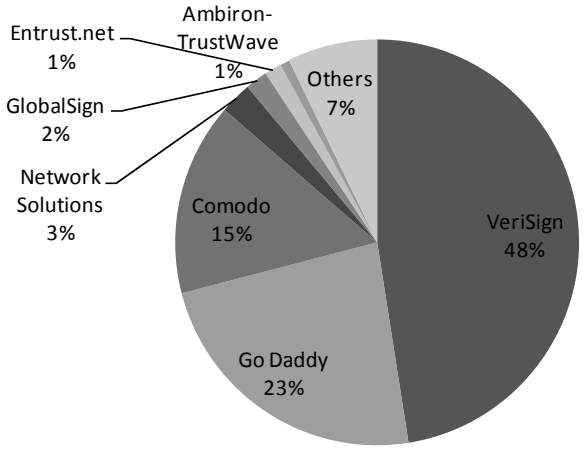
Figure 29. Secure servers per 100 000 inhabitants, July 2010



Source: OECD (2011d) based on Netcraft (*www.netcraft.com*).

Figure 30. . Certificate authority market share, 2009

In number of certificates issued

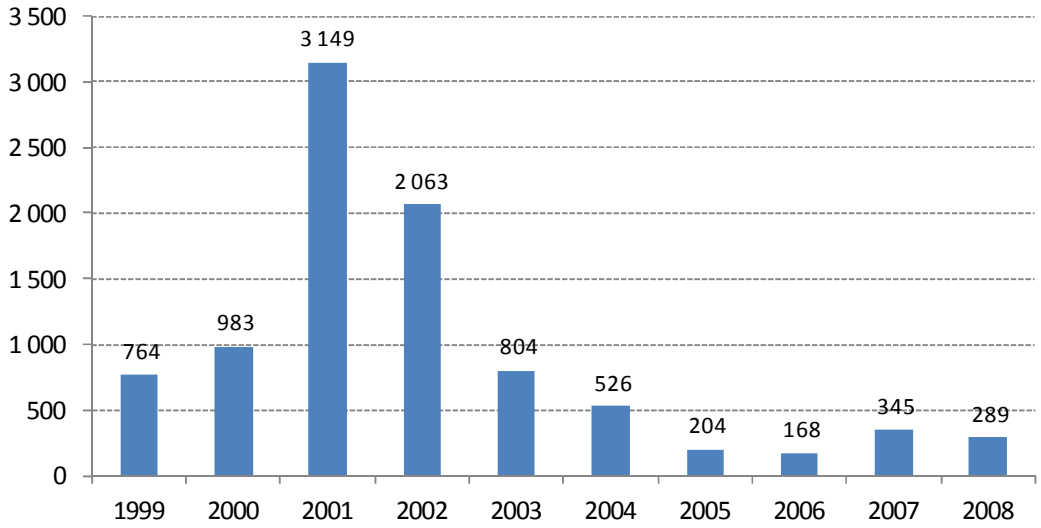


Source: Netcraft (*www.netcraft.com*).

Box 13. Challenges in estimating the costs of cybercrime

The CSI (2008) *Computer Crime & Security Survey* of 522 computer security practitioners in US corporations, government agencies, financial institutions, medical institutions and universities shows that average annual loss reported by organisations in 2008 was just under USD 300 000 (see Figure1). Financial fraud was the cause leading to the highest average loss with an average loss of almost USD 500 000 per organisation in 2008. The second-most expensive security incident was related to botnets that caused losses of nearly USD 350 000 per respondent on average.

Figure 31. Average losses per organisation due to cyber crime in the United States, 1999-2008
In USD thousand



Note: Based on 144 organisations reporting losses of 522 surveys organisations

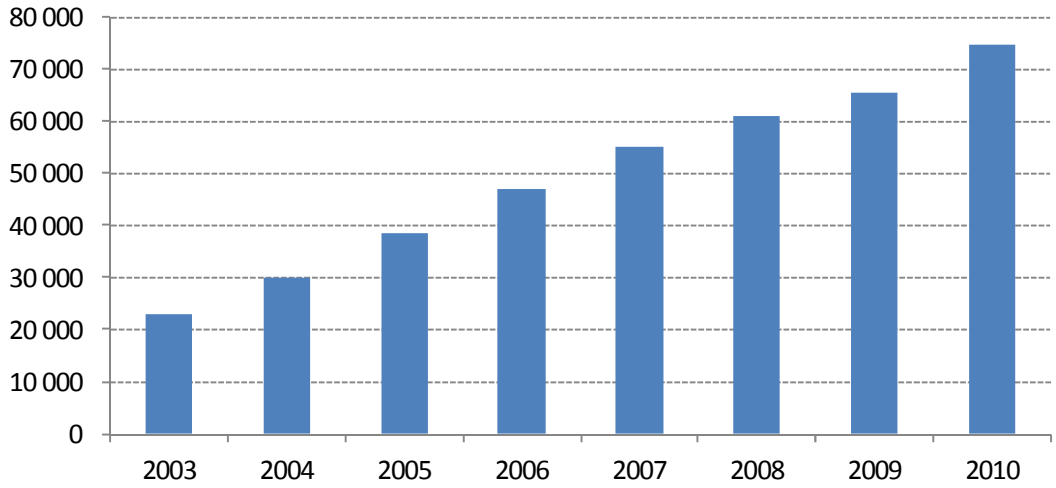
Source: CSI (2008)

There are also very few data on the economic costs of cybercrime on individuals. Examples include the survey commissioned by Symantec (2010), according to which victims of cyber crimes spent an average of 28 days and USD 334 repairing the damage done by cybercriminals. Under the assumption that a victim's time is worth USD 30 per hour (with one hour per day being spent for repairing the damage), that is another USD 840 according to Shinder (2010). This would lead to a total average loss of well over USD 1 000 per user. Other surveys have led to even higher estimations. According to a survey done in 2010 by the Credoc ("centre de recherche pour l'étude et l'observation des conditions de vie"), for instance, more than 50 000 people in France had their computers hacked, causing an average loss of EUR 2 000 (see Lubrano, 2011).

Box 14. Measuring the level of skills in IT security

In 2010, (ISC)^2 had 74 000 certified individuals (*i.e.* members) worldwide (see Figure 312). This is an increase of more than 13% compared to 2009, and the fastest year-on-year increase since 2007. According to a member survey, the average annual salary of (ISC)^2 members increased from almost USD 81 000 in 2006 to almost USD 99 000 in 2010, an average compound annual growth rate (CAGR) of more than 5% per year. The exact number of the surveyed members are unknown, however the distribution of the (ISC)^2 members by country suggests that the figures on average annual salary are most likely biased towards the Americas and the United States in particular.

Figure 312. Number of (ISC)^2 certified individuals worldwide, 2003-10



Source: IISSCC (2011).

PRIVACY

This section analyses indicators and empirical data on privacy that are provided by: (*i*) official statistics agencies, and in particular the *OECD model surveys of ICT use*; (*ii*) other government and public agencies, such as privacy enforcement authorities (privacy authorities) and consumer protection agencies; and (*iii*) non-governmental organisations and data sources, such as the International Association of Privacy Professionals (IAPP), data breach databases and online anonymity and tracking tools. As in the previous section, the matrix presented in Table 1 will be applied for classifying existing and potential indicators where enough data are available.

Official statistics agencies

As is the case for security, national surveys are among of the rare official sources of national statistical agencies for privacy-related indicators. In contrast to security, however, these surveys do not face the same severe limitations due to the lack of technical skills or willingness of respondents to answer correctly in the case of individuals and households. As a consequence, the surveys such as the *OECD model surveys of ICT use* provide a rich and more reliable source for empirical data on privacy.

OECD model survey of ICT use by businesses

The *OECD model survey of ICT use by businesses* includes a number of questions dealing with the topic of IT security and privacy in the context of: (*i*) trust in the online environment, (*ii*) e-business, (*iii*) digitized products, and (*iv*) e-government from a business perspective. Its methodology, scope and coverage have been discussed already in the security section of this report. At this point it should be highlighted that the OECD model surveys include a number of questions used in Eurostat's *Community surveys on ICT usage,* which are mandatory surveys implemented according to regulation (EC, 808/2004).

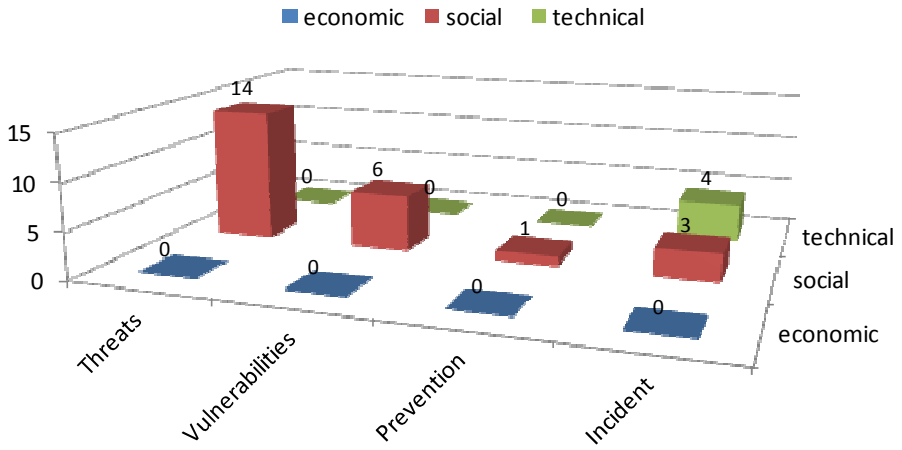
Only two questions of this survey, however, refer to privacy issues. The first one relates to the use of biometric identification techniques, which may infer privacy concerns, whereas the second one concerns the publication of a privacy policy on the businesses' websites, which can be taken as an indication for businesses' awareness of privacy if any.

OECD model survey of ICT use by households/individuals

The *OECD model survey of ICT use by households/individuals* includes a number of questions dealing with the topic of IT security, privacy and trust as barriers for households and individuals. It shares these questions with the Eurostat *Community survey on ICT usage in households and by individuals*, which includes a significant number of questions related to privacy; with 11 out of 19 questions introduced in 2010. Indicators based on the OECD model survey are presented in Box 15.

By systematically mapping all questions related to privacy of the Community Surveys of ICT use by households/individuals into the framework, as done in the previous section, the concentration of existing indicators and gaps in specific areas can be can be highlighted (see Figure 333).

Figure 33. Number of questions related to privacy in the Eurostat Community Survey on ICT usage in households and by individuals, by type of indicator



Source: OECD based on Eurostat, Community Survey on ICT usage in households and by individuals.

The following major observations can be made:

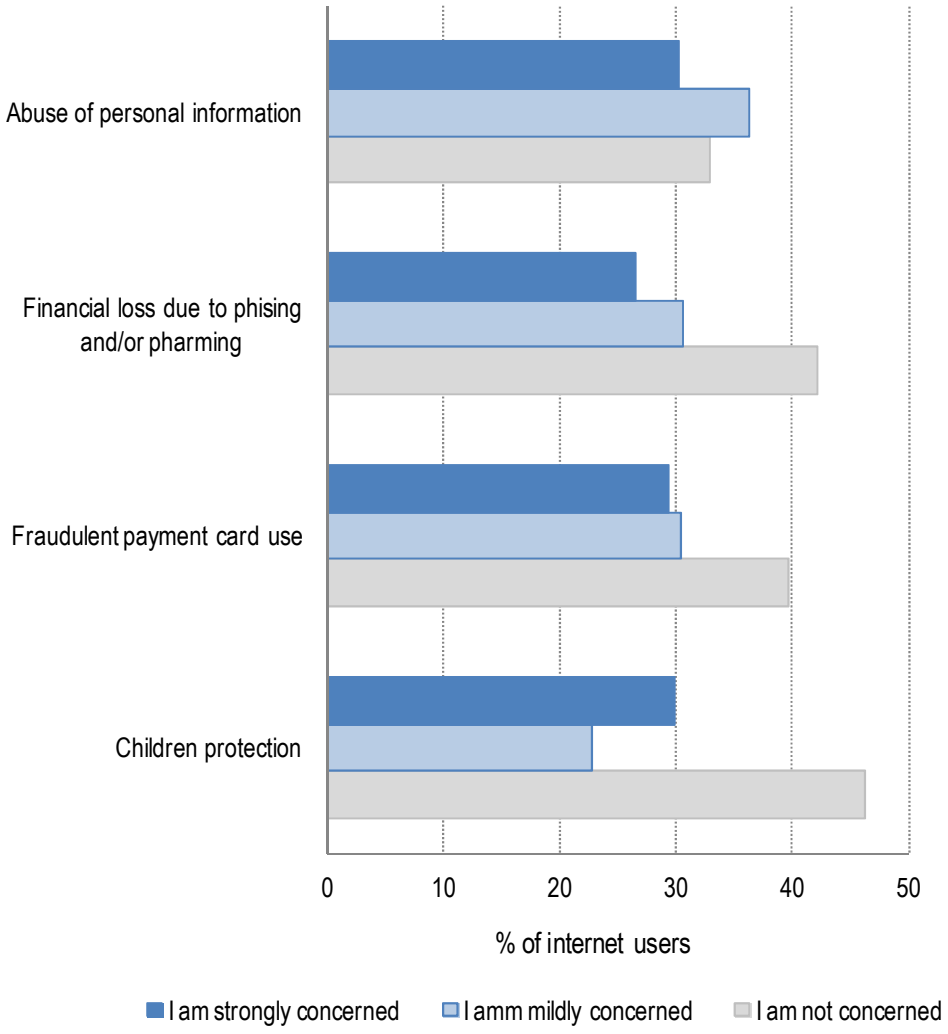
1. Questions related to privacy in the community surveys focus on the social aspects of privacy, with a particular weight on threats and vulnerabilities related to privacy. These include, for instance, all questions related to *e.g.* the awareness of privacy rights (vulnerability) and the privacy-related concerns preventing the use of the Internet (threat).

2. Potential gaps appear in areas related to technical as well as economic indicators. Furthermore, questions related to prevention measures are rare. Questions on the economic impact of privacy violations as well as on the technical measures used to protect privacy should therefore be added to the surveys.

Box 15. Privacy indicators based on surveys of ICT use by households/individuals

Here are some examples of indicators that have been created on the base of the OECD model surveys of ICT use by households/individuals. Figure 9, for example, shows the concerns perceived by internet users on a number of privacy issues. In particular, almost 70% of all internet users are either mildly or strongly concerned about the abuse of their personal information.[49] In addition, Figure 8 in the security section shows the increase, compared to 2005, of the percentage of individuals with Internet access that did not buy on-line, in the last 12 months, for privacy concerns.

Figure 34. Internet user in selected EU OECD countries reporting concern for security and privacy issues, 2010



Source: Eurostat, Community Survey on ICT usage in households and by individuals.

Other government and public agencies

The most promising source for new data sets on privacy comes from government and public agencies other than national statistical offices. In particular, annual reports published by *i*) *privacy protection authorities (privacy authorities)* are a rich source for privacy-related data. Other promising data sets are provided by *ii*) consumer protection agencies on online identity theft. Both are analysed in the following sections.

Privacy protection authorities

The most comprehensive information on privacy and data protection is provided by the privacy enforcement authorities, which are the bodies in charge of monitoring and enforcing privacy laws.[50] These laws may mandate a privacy authority to *i*) secure legal remedies for individuals that have been harmed, *ii*) carry out regulatory audits and inspections, and *iii*) secure compliance by formal legal action of an administrative, civil, or criminal nature, *iv*) advise on legislation or policy initiatives, *v*) cooperate internationally (see OECD, 2006). Other activities may include monitoring attitudes towards privacy (such as through polls and surveys), and undertaking awareness raising initiatives. Annual report and related data by privacy and consumer protection authorities often contain an array of useful data related to these activities.

Annual reports

Privacy authorities issue activity reports on an annual basis. It should be pointed out that these annual reports are official documents, whose drafting and publication is often mandatory.[51] As a result, the data reported refer to those activities the privacy authorities carry out pursuant to the powers they have been endowed with in order to fulfil their role.

Methodology

Despite the commonalities that privacy authorities share, there are variations that have an impact on the comparability of the data set reported by the privacy authorities beyond the remarks made in the general introduction to this report. The problem is well known, and has already been highlighted in OECD (2006):

> "If member country authorities share commonalities in terms of the powers they have and the scope of the laws they enforce, certain variations remain […]. Some authorities are charged with resolving individual complaints, others with supervising regulatory compliance, and many do both. Variations exist with respect to complaint handling processes, the authority to investigate or audit, and the available sanctions and remedies for a breach. Some are independent authorities, some housed within government departments. Some cover the public sphere, others only the private sector and many cover both [...]".

Hence, data on similar functions and tasks are not always reported in a manner that enables comparability. This has implications on many reported data such as, for instance, budget and complaints.[52] Furthermore, not all privacy authorities report the data in a systematic fashion, meaning that the significant data are often scattered in the text and the categories employed are very rarely defined. Moreover, categories evolve in parallel with laws, to the detriment of consistency even within single countries. However, privacy authorities do report information on the same macro-categories. This means that privacy enforcement authorities could co-ordinate their reporting activities to attain the objective of building common data sets to create privacy indicators.

Scope

The current dataset spans a decade, beginning in 2000 and ending in 2010. Since some data protection authorities were established only after 2000, or were in the process of being set up, the sample varies accordingly. Annex TableA.2 shows the date of the creation of the privacy authorities, and the consequent time frame to which the available data relates. Moreover, links to the annual reports are provided in Annex TableA.3. So far, data on a number of OECD countries could not be attained.

Data

At this stage, it has been possible to extract data from the annual reports on the following categories. These categories could be subject for further discussion as their relevance for policy making is not entirely clear:

- **Financial resources allocated** to privacy authorities (income and expenses): This category refers to the financial resources available to the privacy authorities for their functioning. Following the results of the data collection carried out, the sample can be divided into (at least) two groups. The first group encompasses those privacy authorities publishing detailed financial statements, which include at least the percentage of resources given by the government as opposed to their own resources (Italy and Mexico) or donations received (*i.e.* Mexico and Slovenia), as well as expenditure (Australia, Ireland and United Kingdom). The second group includes the privacy authorities which provide a single figure only (overall budget), without explaining its different components.

  Moreover, some privacy authorities have jurisdiction over other issues besides data protection and privacy. For instance, the Mexican Authority is also in charge of ensuring governmental transparency and access to public information. Consequently, these privacy authorities' budget may be overall higher than that of those privacy authorities which do not carry out such additional tasks, and it may not be possible to ascertain the percentage of resources allocated to data protection and privacy activities.

- **Personnel**: This category refers to the total number of people employed by the privacy authorities at the end of each year covered by the annual reports. Not all privacy authorities provide information on turnover; only a few actually provide the average number of employees for each given year.[53]

- **Public outreach**: This includes outreach actions, such as conferences, seminars, press releases, the publication of informative material and targeted guidelines. Currently, only speeches and press conferences are comparable, while information on publications of interest varies greatly. Some privacy authorities, for example, report the number of newsletters published per year.

- **Complaints received and addressed**: Complaints are "allegations about acts or practices that may be an interference with the privacy of an individual" (Australian Government, 2010, p. 50). This usually concerns how personal information is collected, held, used or disclosed by data controllers, whether in the private or the public sector, as allowed by each country's legislation.

  The substantial number of available sub-categories provides multiple opportunities for indicators, but it also magnifies the divergence in reporting. Further analysis needs to be done to clarify, for instance, whether the initial approach to the privacy authority is counted as an information request, or as a complaint, or double counted under both categories. Industry sectors are not equally defined, as well as the alleged violations, which sometimes refer to the law breached, and

other times to a privacy principle. It is understood that few privacy authorities publish all sub-categories.

It should also be noted that the complaints' procedure can affect the comparability of the collected complaint data. Therefore, these procedures need to be assessed to better understand their impact on the generation of data.

Box 16. Understanding the challenges and limitations of complaint data for consumer policy making

Recent OECD (2011h) work on the role of consumer complaints for enhancing policy making highlights that complaint data have an important role to play in policy making. In a survey of 17 OECD countries, a high share of respondents stated that complaint data were important in their policy making process. They thereby highlighted in particular identification of specific consumer problems and the setting of priorities for enforcement actions as important application areas.

However, concerns in using complaint data were also raised in particular in terms of the costs of compiling and analysing the data as well as the validity of complaint information, their classification and comparability across different sources. Furthermore, the report reveals that middle-aged, high income individuals who are well educated are more likely to file complaints. Those who are familiar with consumer rights and have Internet skills are also more inclined to take action. The report also highlights that consumers are more likely to complain if i) the level of detriment is significantly higher; ii) the time and effort to fill the complaint is significantly lower; iii) the complaint processes are significantly more accessible; and iv) the prospects that the complaint will be addressed is significantly higher.

All this highlights that the interpretation of complaint data requires a deep understanding about all the factors effectively affecting the likelihood of filing complaints.

Source: OECD (2011h)

- **Investigations, including inspections and audits:** Complaints often lead to conducting investigations and inspections. Yet, investigations may not necessarily be sparked by a complaint. The privacy authority may investigate, and report data on, a case following the notification of a privacy breach, *i.e.* by whistleblowers, or following media reports, or because they believe there may be a breach. The investigation may be conducted from the desk, entail on-site inspections, or involve the use of evidence-gathering through interviews, depositions, subpoenas and other forms of compulsory legal processes. In addition, most privacy authorities are empowered to carry out audits of certain public or private sectors. "Scheduled audits are intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive. […] Priorities and targets for audit are identified taking account of complaints and enquiries to the Office" (Office of the Irish Data Protection Commissioner, 2010, p. 19). Audits can then inform the provision of informal assistance by the privacy authority.

- **Response to individuals**: This category refers to responses to inquiries from the public and the media. This category refers to the written and telephone queries of individuals seeking information about anything, from their privacy rights to any advice as to how to resolve privacy complaints. It should be noted that it is not always possible to understand whether queries include requests for assistance over specific data protection laws, which pertain to legal opinions and are not considered at this stage of the report. Likewise, in a few instances the data on queries is conflated with that on complaints, making it difficult to compare the data.

- **Number of data protection officers in organisations**: Some privacy authorities report the number of Data Protection Officers (DPOs) named by data controllers. Some also provide statistics on the training sessions offered to these DPOs.

- **International activities, and in particular cross-border co-operation:** Several privacy authorities report the activities they have carried out at the international level (*i.e.* international organisations and working groups). Very few data are reported on the number of foreign individuals requesting help.

Potential indicators

Table 4 lists some potential indicators that could be developed on the basis of the privacy authorities' annual reports data. It should be stressed that these indicators are mainly proposed for further discussion. They would in particular require common definitions of the categories presented in the previous section.

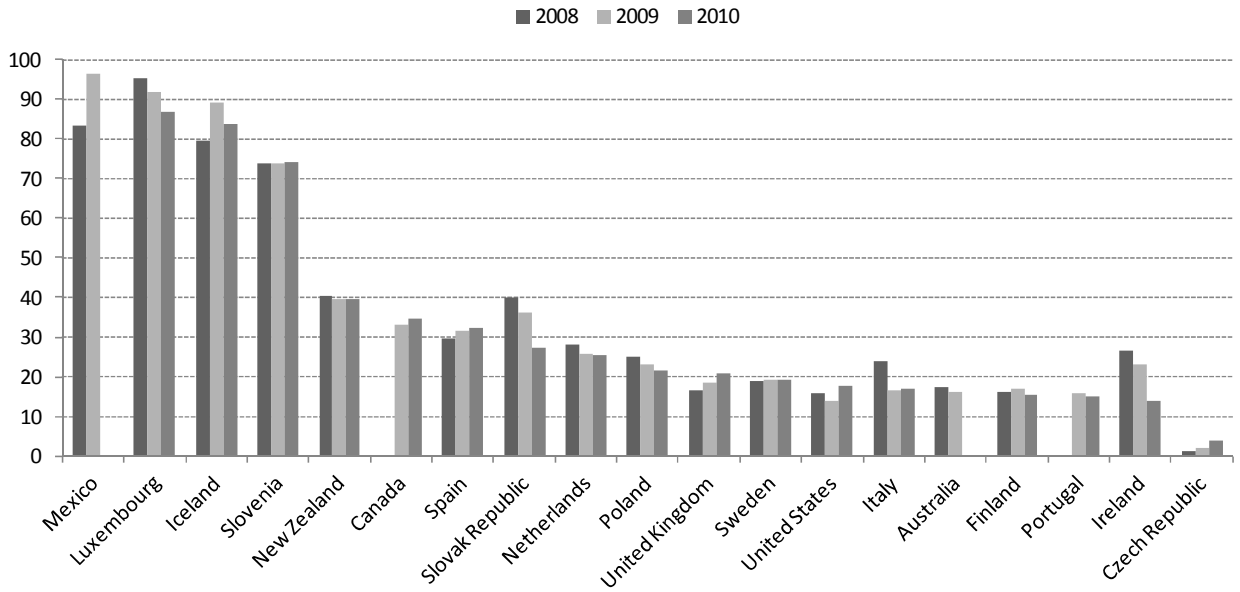
Table 4. Potential indicators from the privacy authorities' report

Indicator	Data source	Possible measurement objectives
*** Budget/GDP ratio** *** Budget/total government budget ratio**	Budget	Economic measure of the government's priority and awareness of the need of protecting citizens' privacy
*** Number of personnel/capita**	Personnel	Human capital resources of the privacy authority; this can be combined with the number of cases received to show the privacy authority's adequacy of resources.
*** Number of public relation activities**	Relations with the public	Can be combined with other activities to estimate the work load of the privacy enforcement authority.
*** Number of complaints received and closed** *** … by sector** *** … by type**	Complaints	Measure of privacy incidents to households and individuals; this can be further refined by taking into account the cases not related to privacy, in order to evaluate individual's awareness of their rights.
*** Number of complaints/capita**	Complaints	
*** Annual growth of complaints** *** … by sector** *** … by type**	Complaints	
*** Number of investigations** *** … on-site inspections** *** … audits**	Investigations	Measure of the response to potential incidents to households and individuals; audits measure prevention by the privacy authority to threats.
*** Number of notifications registered**	Notification	Measure for the risk of privacy violation
*** Cost of data breaches**	Data breaches	Economic measure of privacy incidents
*** Number of registered DPOs**	DPO register	Measure level of awareness for privacy protection in the private and public sector.

Box 17. Privacy indicators based on privacy authority reports

The following figures offer an example of economic indicators based on privacy authorities' budget figures and the OECD data on *total general government expenditure*, that is expenditure by government ministries, agencies and the main administration, including spending for social security, healthcare, education where these are state-operated plus local government where available. The sample is divided into two groups: Figure 35 shows the privacy authorities' financial resources allocated by the state over total general government expenditure. Figure 36 shows the overall budget (including own income) over total general government expenditure, as it was not possible to extract the ratio of states' contribution towards privacy authorities' income.

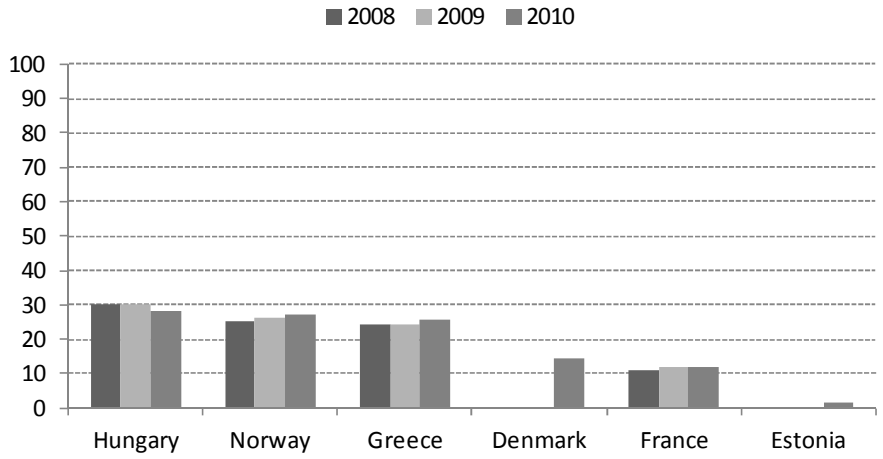
Figure 35. Budget allocated by governments[1] per million of total general government expenditure
National currency



Note: (1) Data Canada and Portugal for 2008 were unavailable.

Source: OECD based on Privacy Authorities' Annual Reports

Figure 36. Overall budget as share of total general government expenditure
Per million, national currency



Note: (1) The figures for Hungary refers to the privacy authority's total expenses
(2) Data on Estonian and Danish resources for 2009 were unavailable

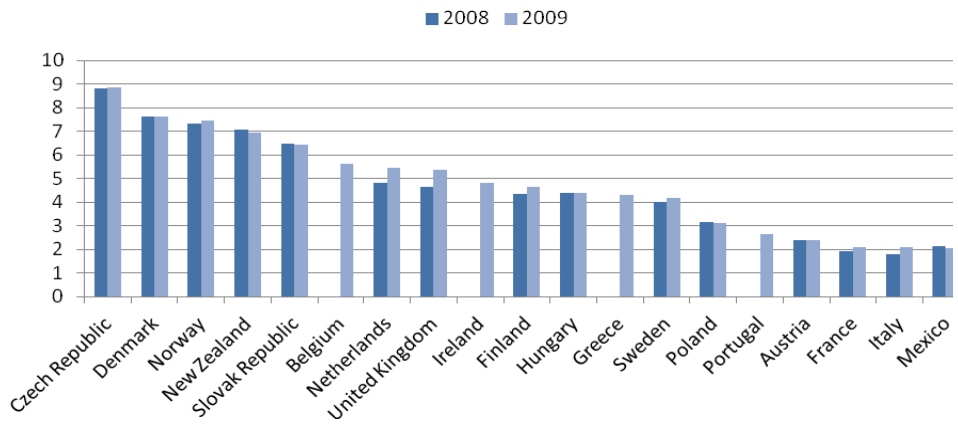
Source: OECD based on Privacy Authorities' Annual Reports.

Box 17. Privacy indicators based on privacy authority reports (cont.)

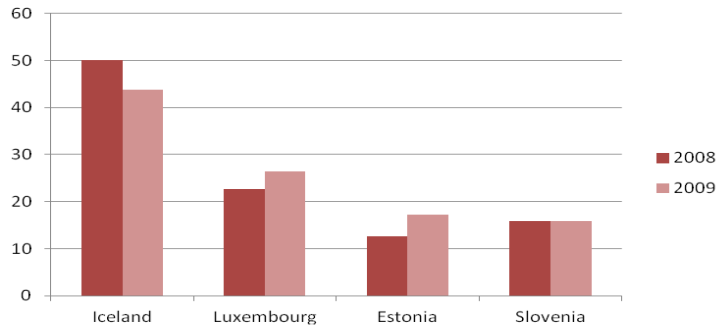
Figure37 is built from the data on personnel provided by the privacy authorities and OECD data. "Personnel" refers to the number of physical employees by the end of the fiscal year calendar (depending on the year of reporting). While full-time positions may provide the base for a better indicator, such information was not available for every privacy authority. It should also be noted that few of the agencies compared are in charge of other tasks, on top of data protection and privacy. The sample is divided into three graphs in order to appreciate the otherwise biasing differences between countries, and in particular the small countries, where the number of employees tends naturally to be higher, as well as the countries which are federal or otherwise organised in two levels of privacy enforcement authorities with the lower level not accounted for here.

Figure 37. Personnel per million inhabitants (A); in small countries (B); in countries with several levels of privacy enforcement agencies (C)

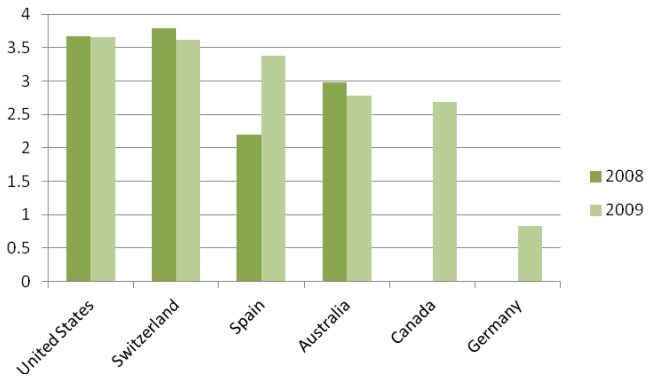
A)



B)



C)



Note (1) the 2009 figures for Belgium, Canada, Germany, Greece, and Ireland are estimated based on weighted average

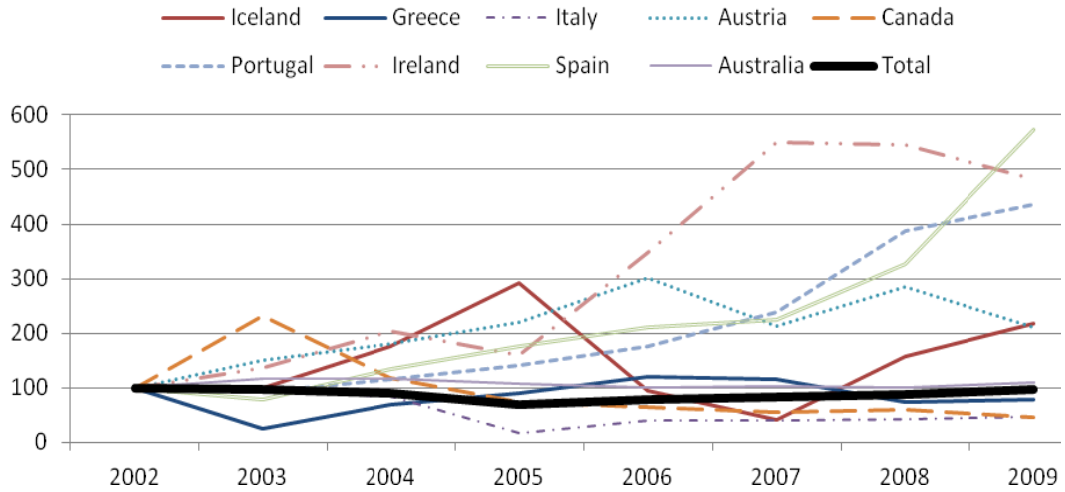
Source: Data Protection Authorities Annual Reports 2008-2009

Box 17. Privacy indicators based on privacy authority reports (cont.)

Figure 3838 shows the trend over time of the number of complaints in selected OECD countries. Complaints refer to alleged violations of, or interference with, the privacy of an individual. As such, complaints can measure the (perceived) privacy incidents to households and individuals. In addition, data relating to complaints can help building very refined indicators, since data are available at different steps of the complaints management procedure. Complaints also contribute to estimating the privacy authority workload. Figure39 shows the share of complaints by sector in 2010 in selected countries.

Figure 38. Complaints trends in selected OECD countries, 2002-2009

Index, 100 = 2002

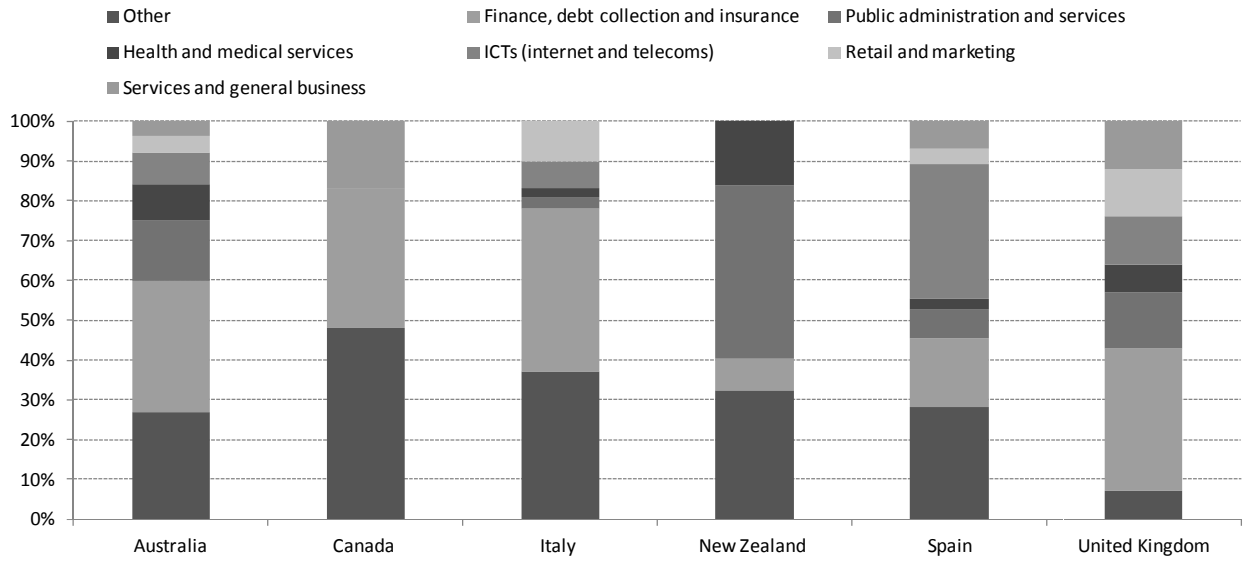


Note: (1) The figure for Iceland refers to complaints, appeals and rulings.

(2) The 2009 figure for Ireland refers to complaints opened for investigation.

Source: Data Protection Authorities Annual Reports 2002-2009, OECD.

Figure 39. Complaints by sector in selected OECD countries, 2010



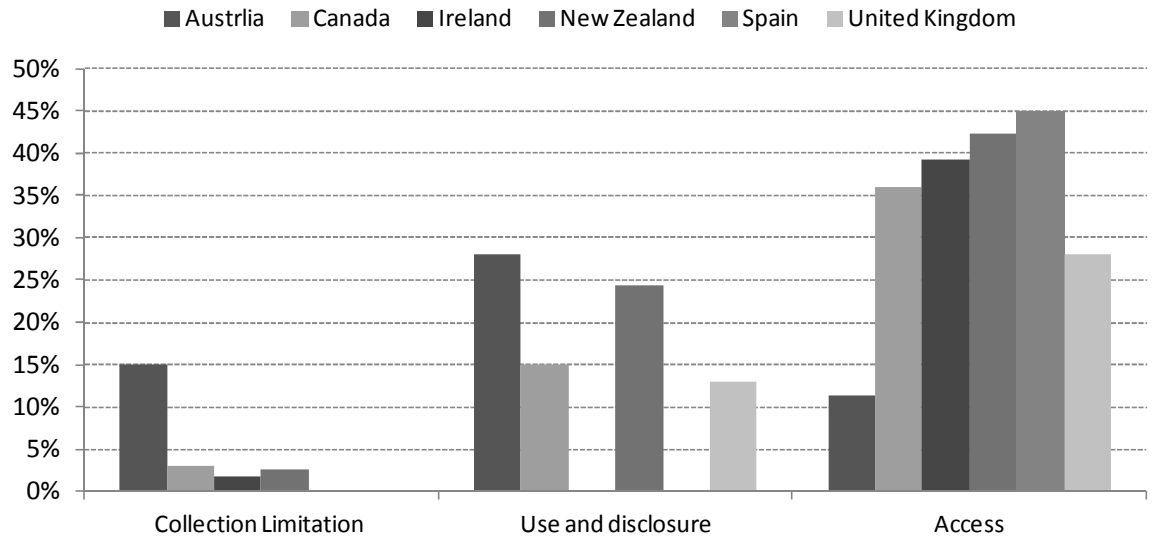
Note: (1) ICT in Spain includes spam

Source: Data Protection Authorities Annual Reports 2002-2009, OECD

Box 17. Privacy indicators based on privacy authority reports (cont.)

Figure40 shows the share of complaints on the principle of access, collection and the use and disclosure of data in selected OECD countries. Figure41 shows the number of complaints related to several issues in Korea from 2007 to 2010. It shows in particular the increase in the number of users perceiving privacy related incidents such as "leakage of personal information" and "non consented use of personal information/release to 3rd party".

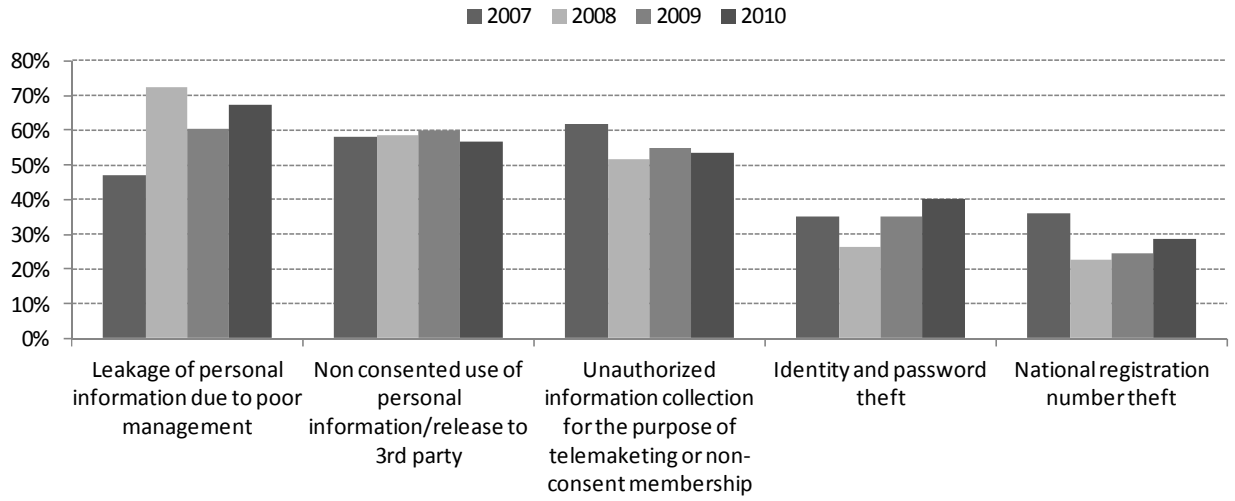
Figure 40. Complaints by type[1] in selected OECD countries, 2010
Percentage



Note: (1) Figure does not include all categories. For Canada data only includes complaints according to the Canadian Privacy Act

Source: Data Protection Authorities Annual Reports 2002-2009, OECD

Figure 41. Complaints by type in Korea, 2007-10
multiple responses, internet users 12 and over



Source: KISA, 2010 Information Security Survey, May 2011

Surveys

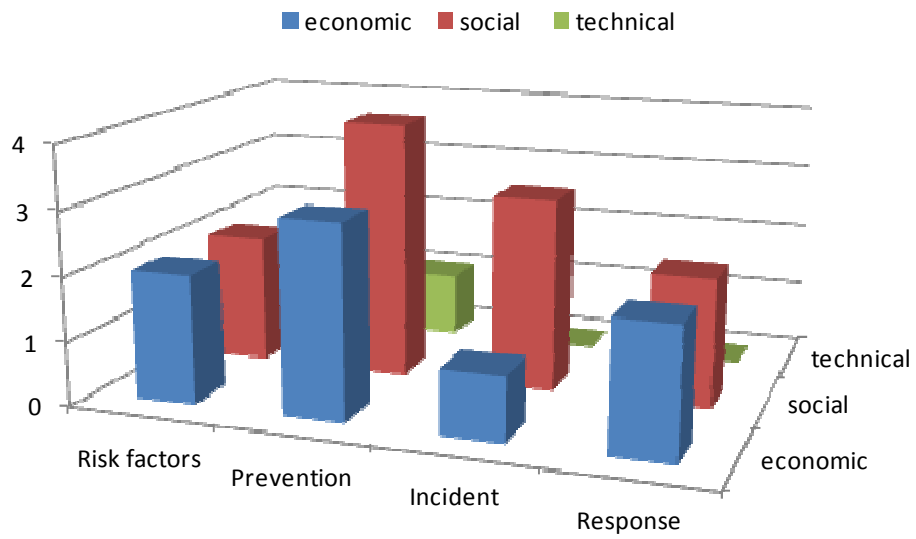
Several privacy authorities have also commissioned opinion polls and surveys to map attitudes towards privacy, or other related issues, in order to better support the awareness raising initiatives they undertake. This information, coupled with information provided by the annual reports, can unveil helpful data to build indicators.

The topics of the surveys vary (see Annex TableA.4). Some privacy authorities try to map public awareness towards privacy (*i.e.* France, Ireland, Israel and Slovakia), others explore the differences in attitude amongst government, businesses, and community (*i.e.* Australia, Canada and Denmark), or youth (*i.e.* Sweden). Moreover, some privacy authorities track the 'customer satisfaction' of those they assisted (*i.e.* United Kingdom), or the public's awareness of the very existence of the privacy authority (*i.e.* France). Finally, some privacy authorities inquired in data security (*i.e.* Canada and Spain), the use of data by police (*i.e.* Norway), businesses' (best) practices (i.e. Poland and United Kingdom) or the use of portable devices (*i.e.* New Zealand). While more examples could be provided, this list may already show how promising this source is, and calls for a detailed analysis of the data, which is scheduled at a later stage of this project.

Gap analysis

Overall, nine macro-categories of data have been identified for privacy authorities, which have been combined into a number of suggestions for indicators, as shown in Table 4. Figure 42 demonstrates that these indicators cover almost all areas defined by the analytical framework. In fact, the privacy authorities' annual reports are one of the rare sources to provide data that can be used to build indicators on the economics of personal data. By collecting additional data available in the annual reports, the coverage of the indicators could be improved.

Figure 42. Number of potential indicators from the privacy authorities' reports by type



One option which could be explored is the idea of developing a 'basket' of weighed activities which are representative of their workload. For instance, privacy authorities could decide on what is a good measure of their tasks, such as responding to queries, drafting opinions, carrying out an audit, etc., and weigh them according to a shared measure.[54] This would be a more reliable way of assessing the adequacy of budgetary and human resources. This measure may also allow to observe correlation between, say, the number of audits carried out and the complaints received, and to evaluate the impact of the preventive measures.

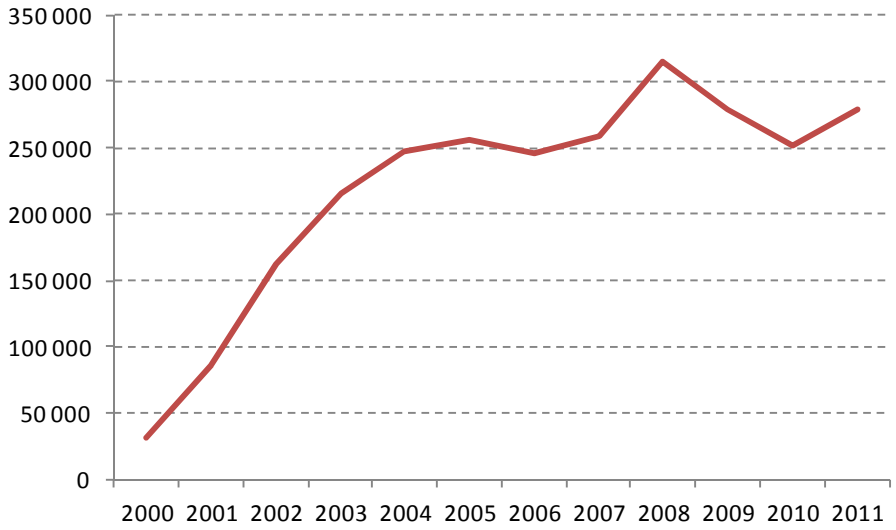
Consumer protection agencies

This section will look at data provided by consumer protection agencies which are related to privacy. This includes in particular statistics on *identity theft* and in some cases also on spam. In particular, the data collected by the FTC's Consumer Sentinel Network (CSN) on identity theft are presented to illustrate the potential of this type of data sets. For more information about the Consumer Sentinel Network, please refer to the section on consumer protection agencies, under the section on security of this report.

Box 18. Privacy-related indicators based on the Consumer Sentinel Database

Figure43 shows the number of complaints related to *identity theft* stored in the Consumer Sentinel Database. Between 2000 and 2011, the number of complaints related to identity theft has increased on average by more than 20% yearly. In 2008, the number of complaints reached its peak with almost 315 000 complaints, but decreased by 11% and 9% year-on-year in 2009 and 2010 respectively. In 2011, the number of complaints increased again compared to the previous year by 11%. As highlighted in Box 6, complaints in CSN are self-reported and unverified, and they do not necessarily represent a random sample of consumer injury for any particular market. For these reasons, year-to-year changes in the number of fraud and/or identity theft complaints do not necessarily indicate an increase or decrease in actual or perceived fraud and/or identity theft in the marketplace.

Figure 43. Number of complaints related to identity theft in the Consumer Sentinel Database, 2000-10



Source: OECD based on U.S. FTC, Consumer Sentinel Network Databook January-December 2011 (Feb. 2012).

Private organisations and data sources

As is the case for security, NGOs, including commercial as well as not-for-profit organisations, are an important additional source for data on privacy. This section will present: *i*) data collected by the International Association of Privacy Professionals (IAPP); *ii*) data on data breaches; and *iii*) data on anonymity tools such as Tor[55] and Ghostery[56]. Other sources such as accounting firms could be included, as shown by some anecdotal evidence presented in Box 19.

Box 19. Some anecdotal evidence related to privacy

Anecdotal evidence is the weakest form of evidence for policy making. However, it can be useful in areas where other evidence does not exist or is not available in the short-term. In this case, anecdotes should be collected and evaluated systematically to assure a certain degree of representativeness.

For example, according to Gomes (2009), privacy-related consulting services provided by law and accounting firms are a USD 500-million-a-year business and have been growing at double digits. And expenses inside companies for privacy compliance easily run into the billions.

International Association of Privacy Professionals

The International Association of Privacy Professionals (IAPP) was founded in 2000, and it is 'the world's largest association of privacy professionals with more than 9 000 members in 70 countries. The IAPP helps define, support and improve the privacy profession through networking, education and certification".[57] The IAPP has realized a number of studies pertinent to the objectives of this report, which can positively contribute to the creation of indicators:

- The 'Data Protection Authorities 2010 Global Benchmarking Survey', which is in its second edition, provides a comparison of a selection of privacy authorities (not all of which are OECD member states' privacy authorities), based on results of a questionnaire (and, therefore, based on data which is not necessarily the same collected here).

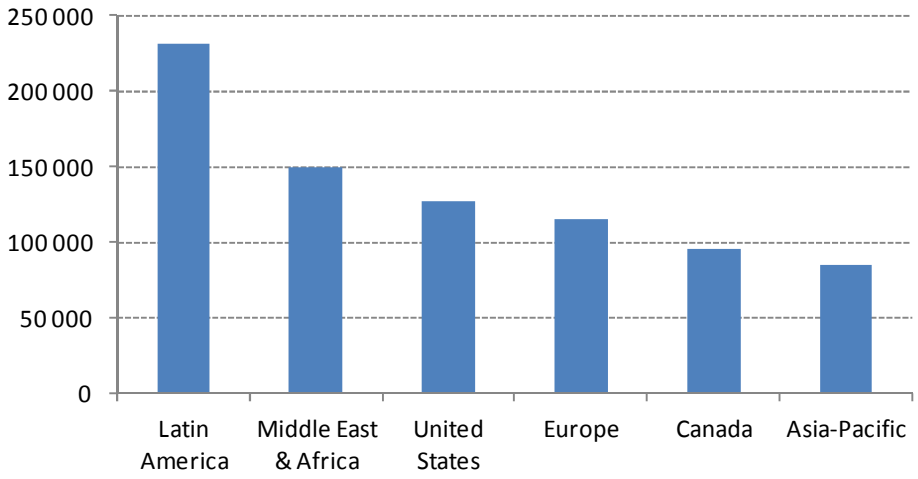
- The 'Call for Agility: the next-generation privacy professionals,' analyses in depth the profession of Data Protection Officers to grasp the main trends. The 'Privacy Professional's Role, Function and Salary Survey' series provides an analysis over time of the privacy profession (see Box 20).

The information contained in these studies represents a valuable complement to the information found in privacy authorities' annual reports, and provides evidence for the OECD project on the economics of personal data.

Box 20. Privacy-related indicators based on reports by the AIPP

Figure44 is taken from the IAPP 2011 Salary Survey including almost 1 000 privacy professional. Figure44 shows the distribution of the average base salary of privacy professionals by region in 2011. It highlights in particular the high salaries of privacy professionals in Latin America as well as in the Middle East and Africa compared to the United States, Europe, Canada and the Asia-Pacific region. However, it should be noted that data for Latin America, the Middle East and Africa, and Asia-Pacific are most likely biased due to the very low samples size. Overall, the average salary of IAPP members, which are mainly located in the United States, increased from more than USD 110 000 in 2010 to USD 124 000 in 2011 (+12%).

Figure 44. Average base salary of privacy professionals by region, 2011
USD



Source: OECD based on IAPP (2011).

Data breach databases

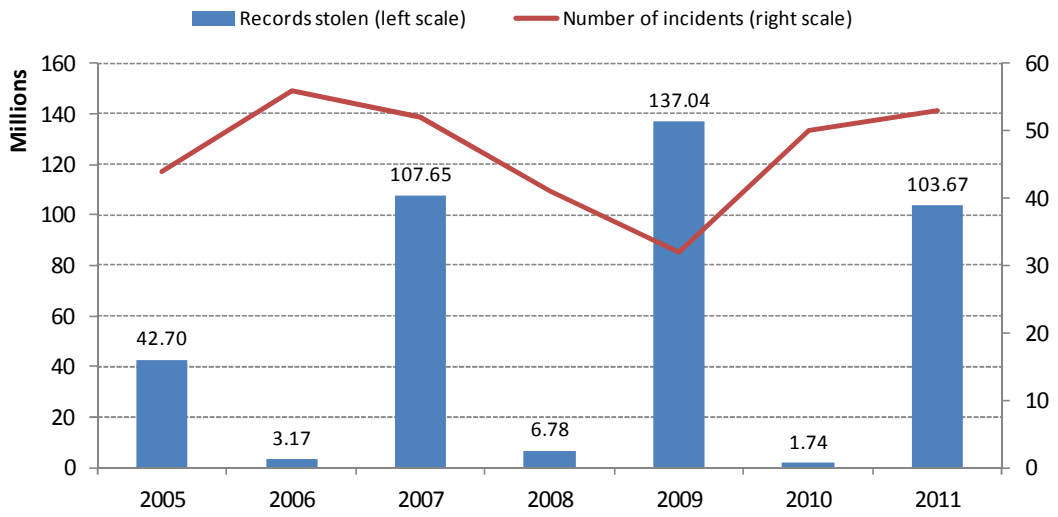
A number of private organisations have gathered information about events involving the loss, theft, or exposure of personal data. The Open Security Foundation (OSF), a "non-profit public organisation founded and operated by information security enthusiasts"[58] provides the DataLossDB dataset for its registered users. It includes data by: *i*) data types (see Annex TableA.5); *ii*) breach types (see Annex TableA.6); and (*iii*) sector. Other NGOs such as the Privacy Rights Clearinghouse (PRC), "a non-profit consumer organisation with a two-part mission – consumer information and consumer advocacy" in the United States, is providing similar datasets partly based on DataLossDB but with data sets related to the United States only.

The biggest limitation of these datasets is that first of all they are biased to specific regions. This could be due to legislation requiring data breach notification or publication of that information. Furthermore, because in some cases the data are collected manually (as in the case of DataLossDB), the recording of data breach events could be biased due to language barriers. A first glance at the distribution of incidents, for example, suggests that *e.g.* DataLossDB may be biased towards English speaking countries and the United States in particular (see Box 21). Even if similar databases exist across countries, there is a high risk that differences in definitions and taxonomies may lead to incomparable statistics. Despite these limitations, data breach data may be useful in understanding the nature of the data breach and some trends over time.

Box 21. Statistics on data breach incidents

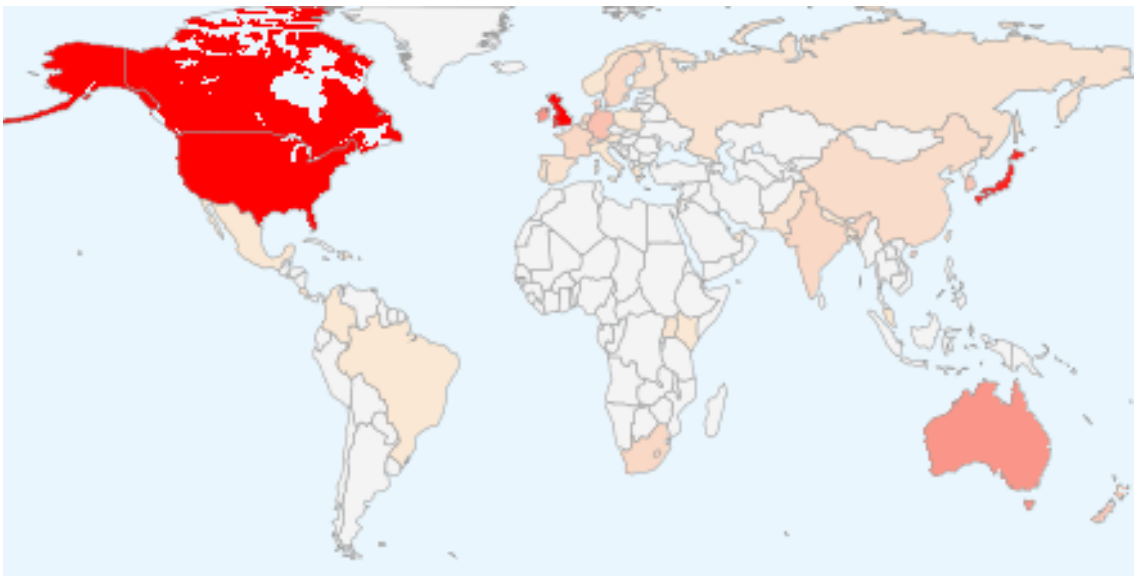
Figure45 shows the number of data breaches incidents by malicious hacks mainly affecting users in the United States between 2005 and 2011. It suggests in particular that the number of incidents identified oscillates around 45 incidents per year, while the total number of records stolen is increasingly determined by large scale data breaches, *i.e.* data breaches involving more than 10 million records (see Figure 45). Malicious hacks still remain the most frequent cause for data breaches in terms of records stolen but not in number of incidents. For example, 63% of all exposed records of incidents recorded by the *Privacy Rights Clearinghouse* between 2005 and 2011 are related to malicious hacks, followed by "lost, discarded or stolen laptops, PDA smartphones, portable memory devices, CDs; hard drives; data tapes, etc" (*i.e.* lost) with 27%. Figure46 shows the distribution of data breach incidents by regions as collected by DataLossDB. It suggests in particular a bias of the data towards English speaking countries.

Figure 45. Data breach incidents by malicious hacks mainly affecting users in the United States, 2005-11



Source: OECD based on data from the Privacy Rights Clearinghouse, *dataloss.db* and *reuters.com*

Figure 46. Hot map of data breach incidents by country, 2011



Source: DataLossDB.

Anonymity surfing and tracking tools

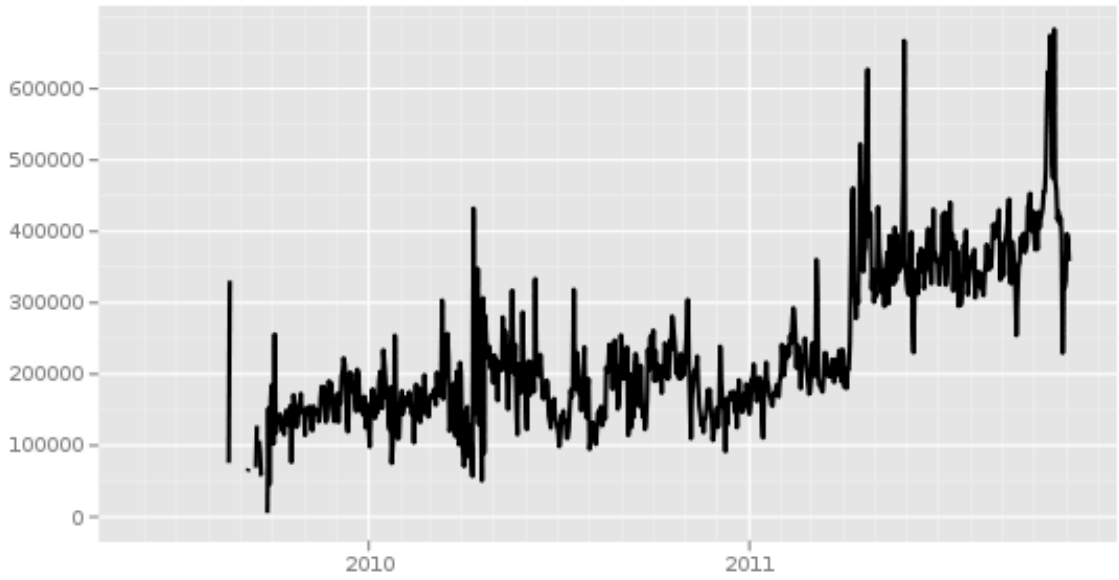
The Tor Project

Tor (originally the acronym for *The Onion Router*) is free software that protects internet users' privacy, confidentiality of communications, and other freedoms (*i.e.* freedom of expression) by enabling online anonymity. The project was initially sponsored by the US Navy Research Lab, then by the Electronic Frontier Foundation, and now by the Tor Project, which is a US based research and education not-for profit organisation, with different sources of funds published on the website. The Tor project makes publicly available the "analytics for the Tor network, including graphs of its available bandwidth and estimated user base".[59] This information could complement the data extracted from the Eurostat surveys, in particular by providing evidence on users' responses to privacy risks. Indicators based on the Tor data are presented in Box 22.

Box 22. Privacy-related indicators based on Tor data

Figure47 shows that the total number of Tor users worldwide has increased from mid-2009 to November 2011. Notable peaks may correlate to particular events in specific countries. Most daily users are located in the United States (almost 75 000 users on average, 19%), followed by Germany (40 000, 10%), Iran (37 000, 9%), France (23 000, 6%), Italy (20 000, 5%), Korea (15 000, 4%), and the Russian Federation (15 000, 4%).

Figure 47. Daily numbers of directly connecting users from all countries, June 2009-November 2010



Source: The Tor Project (*https://metrics.torproject.org*).

Ghostrank

Ghostrank is an anonymous opt-in feature which allows the collection of data generated by the use of the Ghostery browser tool provided by Evidon, which "scans the page for scripts, pixels, and other elements and notifies the user of the companies whose code is present on the page".[60] Ghostrank includes data such as the tracker seen by Ghostery, the domain serving the trackers, whether the tracker was blocked or not, the GhostRank user's country of origin and the browser in which Ghostery was installed. This information could complement the data extracted from the Eurostat surveys, in particular by providing evidence on users' responses to privacy risks, as well as on businesses attitudes towards enabling privacy settings in compliance with privacy laws.

The data collected by Ghostery could suggest very useful information on: the number of trackers encountered by the average Ghostery user over time; the number of trackers blocked on average, as well as how often the users did not block trackers; whether there is a correlation between the country of origin and the rate of consensus/blocking; the sectors tending to send the most ads; the number of advertisers and their vendors honouring the opt-out requests once they have been contacted by Ghostery, and whether there is a variation according to the sector. As stressed for the Tor software, this information could complement the data extracted from the Eurostat surveys, in particular by providing evidence on users' responses to privacy risks, and on business practices towards privacy.

Table 5. lists potential privacy indicators from NGOs that are proposed for further discussion.

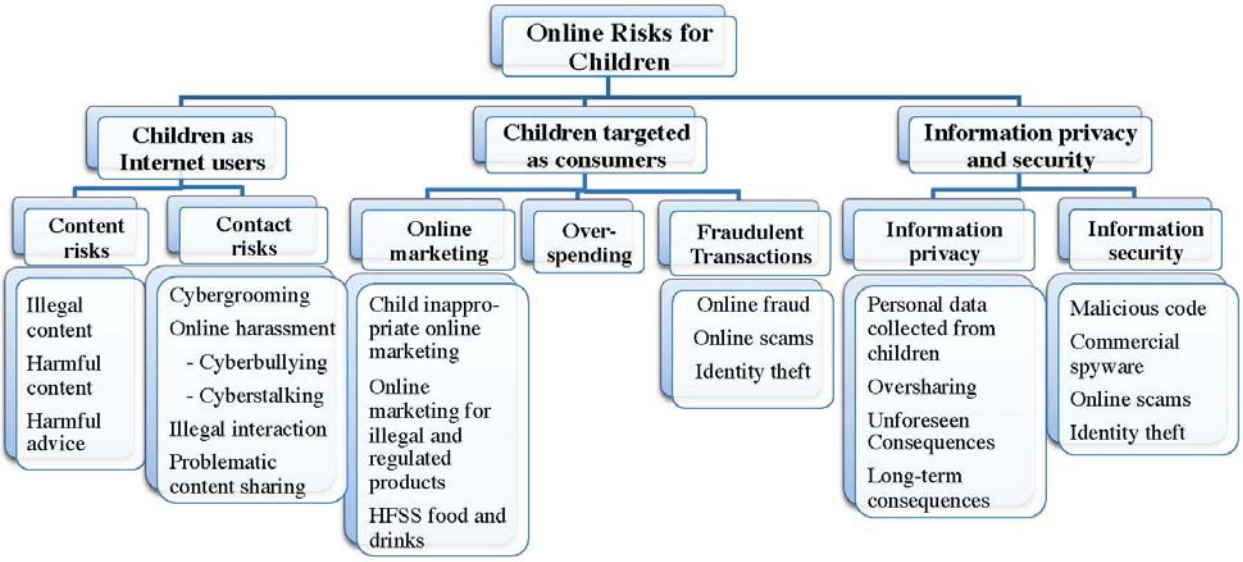
Table 5. Potential privacy indicators from NGOs

Indicator	Data source	Object measures
*** Variation of data protection officers /chief privacy officer salaries worldwide**	IAPP salary survey	Economic measure of businesses prevention of privacy incidents
*** Increase in IAPP membership (DPOs/CPOs)**	IAPP members	Social measure of businesses prevention of privacy incidents
*** Increase in TOR use**	Tor users	Social measure of users' awareness (prevention) of privacy risks
***Number of trackers allowed/blocked by Ghostery users**	GhostRank data	Social measure of users' response to privacy risks
*** Ratio of companies which honour/ do not honour the op-out requests**	GhostRank data	Social measure of the businesses attitude towards respecting privacy rights
*** Most common sectors where the opt-out requests are not honoured**	GhostRank data	Social measure of the businesses disrespect (incident) of privacy rights

PROTECTION OF CHILDREN ONLINE

This section analyses indicators and empirical data related to the protection of children online. As discussed in the OECD (2011f) report on *Protecting Children Online: Risks Faced by Children Online and Policies to Protect Them*, the risks that children face online are partly related to information security and privacy. Besides that, children are facing risks online *as Internet users* and when *targeted as consumers* (see Figure48). Thus, indicators presented in the two previous sections can be applied for making policies for the protection of children online if adjusted accordingly. This is possible where indicators on security and privacy can be broken down by age as in the case of *e.g*. the *OECD model survey on ICT use by households and individuals*.

Figure 48. Typology of risks for children online



Source: OECD (2011f)

As in previous sections, this section will look at *i*) official statistics agencies, in particular the *OECD model surveys of ICT use by households and individuals* for the statistics related to children as Internet users as well as security and privacy related to children. It will then analyse data provided by *ii*) other government and public agencies, such as privacy enforcement authorities and consumer protection agencies which have collected data on the privacy of children, and on children as consumers, respectively. Finally, the last section on *iii*) the private organisations and data sets will look at alternative data that can be used to supplement existing data sets. This includes, for example, data on access control software and hardware as well as data on children-friendly web content.

Official statistics agencies

OECD model survey of ICT use by households/individuals

One of the advantages of the *OECD model survey of ICT use by households/individuals* is that it allows building indicators on privacy and security that are specific to age groups. However, this is only possible to a limited extent, since the scope of individuals is currently set to 16-74 years (see previous sections). This means that all statistics on security and privacy developed from the *OECD model survey* can be used for measuring online risks for teenagers (aged 16 to 18 years).

Besides the questions related to security and privacy, a small number of questions in the OECD model survey are specific to the protection of children online. These questions are listed in Table 6 and potential indicators derived from these questions are presented in Box 23. It should be noted, however, that these questions may not yield the most useful information about policymaking interventions to protect children online. This is because the respondents' answers may be influenced by sensational press stories rather than actual experiences. Furthermore, with increasing use of mobile devices by children, which is quickly outpacing their use of household computers, these questions may not capture the most important trends.

Table 6. Survey questions related to the protection of children online

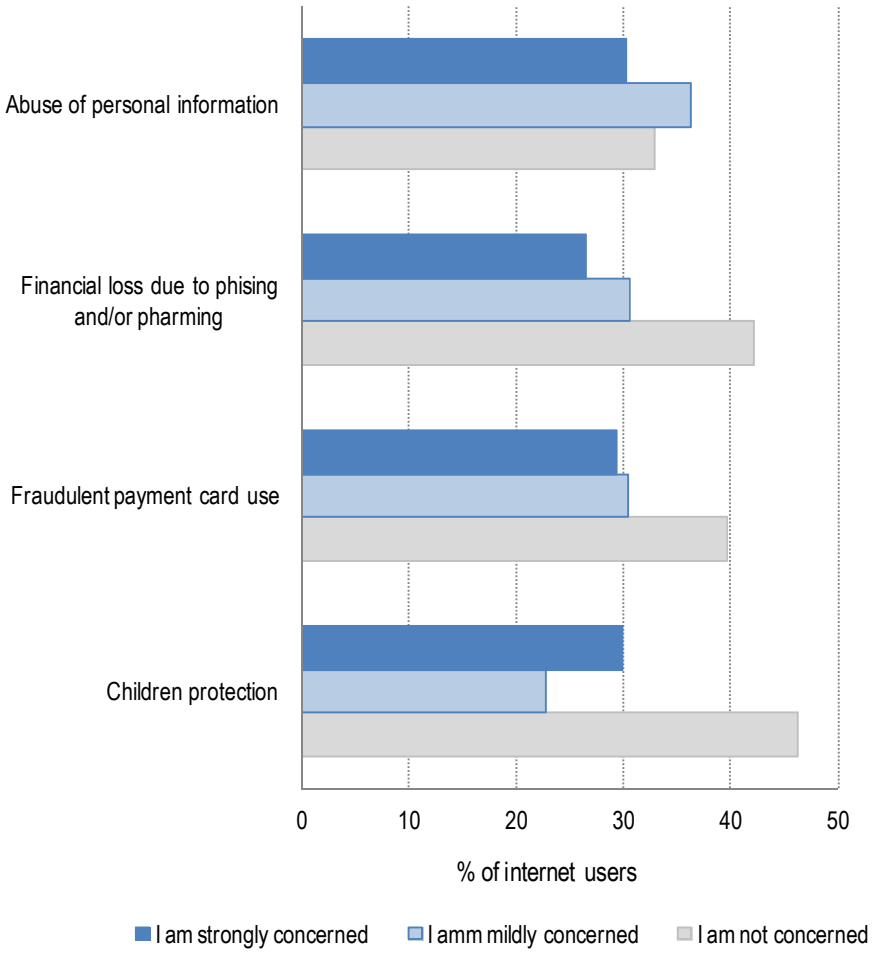
ID question	Year	Question
i_scchldm	2010	I'm mildly concerned about children accessing inappropriate web-sites or connecting with potentially dangerous persons from a computer within the household
i_scchlds	2010	I'm strongly concerned about children accessing inappropriate websites or connecting with potentially dangerous persons from a computer within the household
i_scpchld	2010	I'm strongly concerned about and I have experienced in the last 12 months children accessing inappropriate web-sites or connecting with potentially dangerous persons from a computer within the household
i_secchld	2010	I have experienced in the last 12 months children accessing inappropriate web-sites or connecting with potentially dangerous persons from a computer within the household
i_scpc	2010	As IT security software or tool, I use a parental control or a web filtering software

Source: Eurostat, Community Survey on ICT usage in households and by individuals

Box 23. Indicators on children online based on surveys of ICT use by households/individuals

The following indicators are examples that have been created on the base of the OECD model surveys of ICT use by households/individuals. Figure49, for example, show the concern perceived by internet users on a number of privacy related issues. As for children protection online, 30% of individuals are strongly concerned about the issue, while more than 46% are not concerned. Children protection thus ranks second after the abuse of personal information as a reason for strong concern (but not overall concern).

Figure 49. Internet users in selected EU OECD countries reporting concern for children protection, 2010

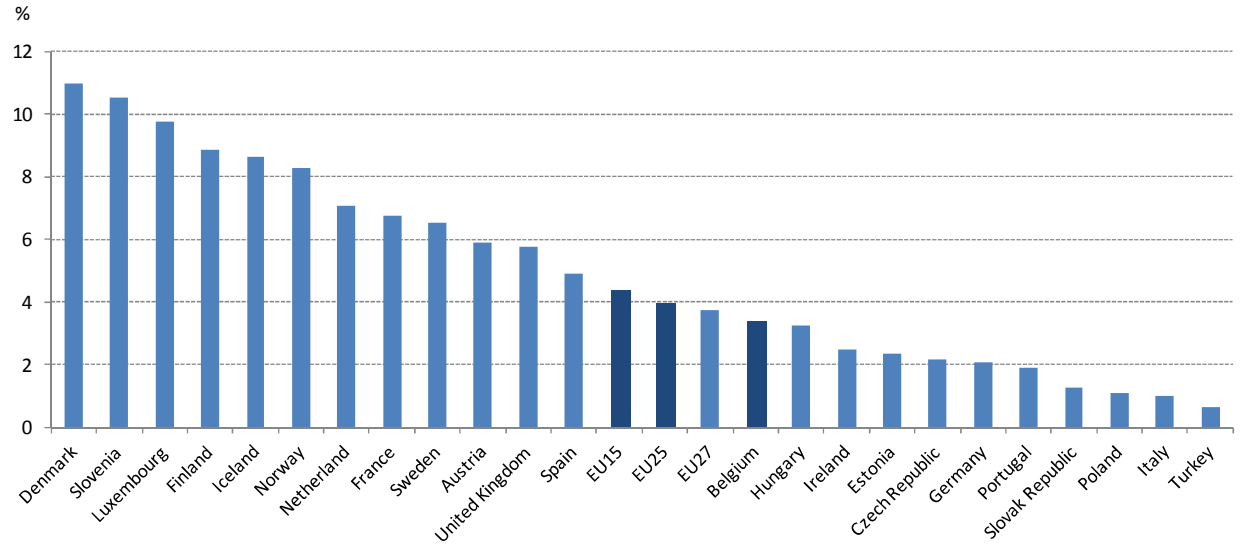


Source: Eurostat, Community Survey on ICT usage in households and by individuals

Box 19. Indicators on the protection of children online based on surveys of ICT use by households/individuals (cont.)

Figure50 shows the share of individuals using a parental control or a web filtering software in OECD Europe. The share is relatively high (above 8%) in Denmark, Slovenian, Luxembourg, Finland, Iceland, and Norway, whereas it is below 2% in Portugal, Slovak Republic, Poland, Italy, and Turkey.

Figure 50. Share of individuals using a parental control or a web filtering software, 2010



Source: Eurostat, Community Survey on ICT usage in households and by individuals

Other government and public agencies

The following section presents potential data sources available at other government and public agencies. This includes, in particular, privacy and consumer protection authorities having children specific data. Furthermore, some ministries such as the Ministry of Internal Affairs and Communications in Japan are currently creating expert group to works indicators regarding the Internet literacy of children. This would in particular include the development of tests that would measure the abilities to cope with overall online risks for children. It can be expected that these tests would enrich the available evidence base for policies on the protection of children online.

Privacy protection authorities

Privacy authorities acknowledge the higher exposure of children or young people's privacy, due to their wide deployment of the internet and of online services, as well as the common stereotype whereby youngsters would care less about their privacy. This is why, in the past couple of years, privacy authorities' reflections and initiatives targeted at raising children's awareness of the risks to privacy posed by the online environment have multiplied. Table in the Annex roughly tracks privacy authorities' approach to the subject at the beginning (2000) and at the end (2010) of the reporting period. 'N' stands for 'no action reported/subject not discussed,' whereas 'Y' refers to 'actions reported/ subject discussed'. The variable is a weak proof of awareness or activity, as the agencies may have simply not reported the information.

Actions vary. The school is obviously one of the main channels employed by privacy authorities to deliver awareness-raising material.[61] Some privacy authorities also target parents as the best guide and control for the youngest children, and have released guides and toolkits. Many privacy authorities then use their websites to publish material, including magazines, dedicated to the young public, some opened a new website designed for children, and a few even opened an account on a social network site such as Facebook and Twitter. Some privacy authorities have directly involved the young public, by having them discuss and realise material aimed at raising awareness among their peers, or by creating privacy-related contests (*i.e.* video contests) with prizes. All these activities could be used to create variable to measure activities of privacy authorities to protect children online.

Consumer protection agencies

Consumer protection agencies can collect statistics on the violation of the rights of children as consumers. However, there are few statistics available and rare are those that are internationally comparable. The FTC, for example, collects and provides information on action law suits against firms violating children's privacy online.[62] As of October 2011, the FTC garnered more than USD 6.2 million in civil penalties. This includes cases such as the one against Xanga.com, a popular social networking site that was penalised to pay USD 1 million for having knowingly collected personal information from, and created blog pages for, 1.7 million child users – without first obtaining their parents' permission.[63]

Most available data are rather based on single studies partly conducted by consumer protection agencies as highlighted in OECD (2011f). For example, a study by the British National Consumer Council (now Consumer Focus) and Childnet International of commercial activities on websites favoured by children shows that 9% of the ads are for online gambling and 4% for dating services (Fielder *et al.*, 2007, p. 11).

Non-governmental organisations and data sources

As is the case for security and privacy, NGOs, including commercial as well as not-for-profit organisations, are an important additional source for data on the protection of children online. This section will present data on access control software and hardware vendors, in particular revenue trends. It will then look at the number of online platforms dedicated to children only. Both numbers are considered to measure the level of awareness by parents and businesses for the need to offer children a safe web experience.

Parental control and web filtering software vendors

Numbers on sales of parental control software can be a additional indicator for the deployment of these tools. This includes for example: *Net Nanny*[64] by contentwatch, CyberPatrol *Parental Controls,*[65] and *Safe Eyes*[66] by McAfee (Intel). The biggest challenge here, however, is that these data are typically not published by these firms, in particular since parental control software are not the core of their businesses (as in the case of Intel) or because there is no report on financial activities at fine enough granularity. Collaboration with these private organisations would therefore be required in order to assess the use of these tools in the policy making process.

Children friendly web content

Statistics on children friendly web content, can provide a proxy on the level of threats faced by children online. Companies such as websense that are providing web filtering solutions as well as search engine operators such as Google, Yahoo! and Microsoft are in a good position to collect and provide statistics on adult-only web content. Again collaboration with these private organisations would be required in order to assess the threats faced by children online in the policy making process.

UNDERSTANDING THE POLICY MAKERS' NEEDS

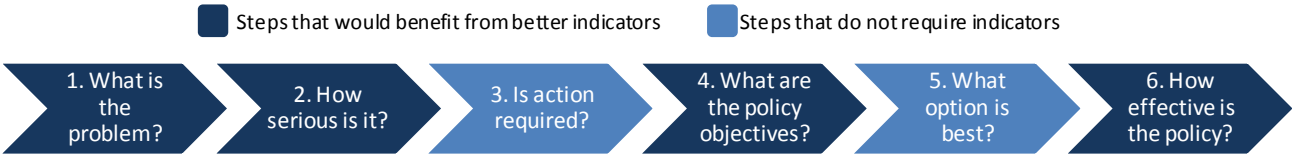
As highlighted by the analytical framework presented in Table 1, policy makers in the areas of information security, privacy and the protection of children online share one common need, namely the need for better assessing the risks faced online. This includes in particular measuring the following risk factors presented in the analytical framework: i) threats; ii) vulnerabilities; iii) impact; iv) prevention and v) response. It therefore can be expected that policy makers in the areas of information security, privacy and the protection of children would benefit from indicators measuring these factors in order to inform their policy making process. However, the need for indicators can vary depending on the problem calling for policy intervention as well as the stage of the policy making process itself. In some situations, anecdotal evidence can be enough to identify and define the policy problems. In other situations, the assessment of economic and social indicators and the analysis through econometric models may be necessary.

This section identifies the types of indicators needed for the policy making process in the areas of information security, privacy and the protection of children online. It presents the main steps of the policy making process as adapted from the OECD (2010d) *Consumer Policy Toolkit*, highlighting in particular those steps where policy makers would benefit from better indicators, and what type of indicators would most likely be needed. Finally, it highlights where indicators are not available or where they are available but would require further efforts to increase the quality, in particular in terms of comparability, building on the analysis presented later in the report.

Steps of the evidence-based policy making process[67]

The OECD (2010d) *Consumer Policy Toolkit* provides a framework for consumer policy decision making which can be adopted for policy making in the areas of information security, privacy and the protection of children online. Its six steps are presented in Figure 51 and in the following sections respectively. The policy making steps benefiting from better indicators for policy makers are highlighted.[68]

Figure 51. Policy making steps



Source: OECD (2010d) Consumer Policy Toolkit.

1. Identifying and defining the problem and its sources

The first step in the policy making process is to identify whether there is a problem that would require policy intervention as well as the relevant stakeholders related to the problem. There are a number of sources that can provide an indication for possible problems. In some cases, this can be done by anecdotal evidence, in particular when similar anecdotes start emerging for example through the media. Policy makers can, however, detect the emergence of problems earlier, for instance, by monitoring activity-related data of government agencies. This is particularly the case with complaint data as collected for example by privacy protection authorities. As will be shown later in the report, complaint data collected by privacy

protection authorities can not only help provide information on the type of problem, but can also help identify relevant stakeholders. In the area of information security, incident data collected by CSIRTs have also the potential to help policy makers indentify problems and relevant stakeholders as will be discussed later in the report.

During this first step, the analytical framework proposed in Table 1 can be used to further define the problem, namely by narrowing down the problem along the two most relevant dimensions of the framework: *i*) risk factors (threats, vulnerabilities, impact, prevention, and response); and *ii*) actors (governments, businesses, individual and households). Once the problem has been indentified and defined according to the framework's dimension, the relevant indicators required for the next policy making steps can be identified based on the framework (see next step).

2. Measuring the risk and the severity of the potential harm

The second step in the policy making process is about measuring the magnitude of the identified potential harm. This step requires the use of indicators and includes in particular assessing the economic and social impacts of potential harms as measured for example by direct financial losses, time loss and loss of trust. It is during this second step that the analytical framework proposed in Table 1 can help policy makers to identify the indicators required to measure the magnitude of the problem. This is in particular the case, if the problem areas have been narrowed down during the first steps to specific *i*) risk factors (threats, vulnerabilities, impact, prevention, and response); and *ii*) actors (governments, businesses, individual and households).

Furthermore, economic and social indicators are most likely to be used during this step of the policy making process, because it is during this policy making step that assessing the economic and social impacts of potential harms becomes necessary. In addition to complaint and incident data discussed in the previous step, survey data and econometric models can provide the necessary insights for assessing the social and economic impacts of potential harms. However, the harm can sometimes be difficult to quantify, in which case the potential harm will need to be assessed in a qualitative manner.

3. Determining whether the risks warrant policy response

The decision whether the risks warrant policy response will be based on the assessment conducted in the previous steps. If the available evidence base indicates that policy intervention is required a policy action should be taken (proceed to step 4). However, policy makers can also decide that more evidence would be required before undertaking a policy action, in which case the previous step would need to be repeated. If, however, the scope of the problem turns out to be too narrow or too broad, the policy making process would have to start again at the first step. In the case that no policy intervention would be required, the policy making process would end here.

4. Setting policy objectives and identify the range of policy actions

When setting policies, policy makers should specify clear policy objectives in terms of what the policy intends to achieve. Appropriate success indicators should therefore be determined in order to be able to evaluate the to effectiveness of the policy (in step 6). Here again the framework proposed in Table 1 can help identify the relevant success indicators. For example, policies targeted to improving the ability of Internet participants to better respond to threats online should include response-related indicators as identified by the analytical framework. Depending on the specific policy the success indicators could be limited to technical, social or economic indicators. In any case, "if metrics are employed, efforts should be made to establish a baseline prior to implementing a policy" (OECD, 2010d).

5. Evaluating and selecting policy options

Once policy options have been identified, the most appropriate and cost effective method for achieving the policy objective (from step 4) needs to be determined. In most cases, a cost-benefit analysis should be carried out, covering both quantifiable aspects and those areas where quantification may not be practicable (*e.g*. community values and ethical considerations). The scale and depth of the analysis should be determined on the basis of the likely consequences of the policy under consideration. This would be particularly the case for "policies that entail high costs on some stakeholders and are of a relatively permanent nature (*e.g*. locked in by legislation)" (OECD, 2010d).

6. Developing a review process to evaluate the effectiveness of the policy

Regular reviews of policies serve to determine if the objectives (set at step 4) are being achieved in a cost-effective manner. The review process needs to factor in changes in the nature of the problem, changes in the environment, and potentially unforeseen or unintended consequences of the selected policy action. The review should take place after a policy has been in operation for a reasonable period of time.

Post implementation evaluations can range from interim monitoring to full-scale reviews. The methods for carrying out reviews are similar to those used for prior assessments of expected costs and benefits. This means in particular that indicators identified in step 2 can be reused for evaluating if a measure should be maintained, modified or eliminated, and whether enforcement should be strengthened or alternative policy actions should be considered. In some cases the nature and source of the problem would need to be reassessed, in which case the policy making process would reiterate to the first step.

Identifying the gaps for the policy making process

As highlighted in the previous section, indicators have an important role to play in the policy making process. Once the policy making process is initiated (step 1), for example by a repetition of incidents or complaints, it needs to be supported by indicators, in particular by economic and social indicators to better assess the potential harms (step 2), to define measurable policy objectives (step 4), and to assess their achievements (step 6). Depending of the scope of the problem identified and defined initially (in step 1), the need for indicators can cover the whole range of the analytical framework, namely all risk factors (threats, vulnerabilities, impact, prevention and response) or it can focus on specific risk factors such as for instance, prevention. The following section presents the availability of data and statistics in the areas of information security, privacy and the protection of children online respectively and the quality of available statistics in terms of comparability. It is based on the analysis presented earlier in the report.

Information security

The assessment of the indicators presented in this report, reveals that comparable statistics are not available across all fields of the framework (see Table 7). In particular in the area of response, no statistics were available. Furthermore, economic as well as social indicators were also rare despite the need for these types of indicators in the policy making process (see step 2). Most comparable statistics in the area of security are provided by national surveys conducted by international organisations such as the Eurostat and the OECD through its model surveys on business and household use of ICTs. These data sources, however, tend to relate to the impact and prevention of security incidents. Other sources providing comparable statistics include the private sector on *e.g.* (technical, threat and impact) statistics on attack traffic and (economic prevention) statistics on R&D related to security. CSERTs were the most promising sources for statistics as the data cover all risk factors (threats, vulnerabilities, impact, prevention, and response) although only from a technical perspective. However, due to limits in the comparability of these data across countries, they can hardly be used for the policy making process in their current state.

Table 7. Availability of comparable statistics related to information security

	Threats	Vulnerabilities	Impact	Prevention	Response
Economic				L	
Social	L		L	L	
Technical	L	L	H	H	

Note: (H)igh if more than 20% of all discovered indicators are related to a specific field. (L)ow if less than 10% of all discovered indicators are related to a specific field.

Privacy

In the case of privacy indicators assessed and presented in this report, comparable statistics are mainly available when they relate to the social dimension (see Table 8). Model surveys are the main source for cross-country comparable statistics in this area, with a high number of questions related to threats observed by individuals and households followed by impact related questions. As in the area of security, comparable statistics related to response were not available. Comparable economic statistics were also not available, which limits the possibility for policy makers to fully assess the impact of privacy threats during the policy making process as described above (see step 2). Statistics collected by privacy authorities were the most promising input for the policy making process in the area of privacy. However, as in the case of CSERT data, privacy authorities' data can only be used to a limited extent due to limitations in interpreting and comparing the data, notably the complaint data. So further efforts would be required to make use of these statistics for the policy making process.

Table 8. Availability of comparable statistics related to privacy

	Threats	Vulnerabilities	Impact	Prevention	Response
Economic					
Social	H	L	L	L	
Technical			L		

Note: (H)igh if more than 20% of all discovered indicators are related to a specific field. (L)ow if less than 10% of all discovered indicators are related to a specific field.

Protection of children online

The development of indicators on the protection of children online benefits considerably from statistics on security and privacy where there is a breakdown by age groups. These statistics almost exclusively come from national surveys conducted by international organisations such as Eurostat and the OECD through its model surveys on household use of ICTs. It is therefore no surprise that there is a relatively high concentration of comparable statistics related to threats from a social perspective and impact and prevention from a technical perspective, as these were the areas where security and privacy related indicators were available (see Table 9). The first and the latter type of statistics, in particular, are very promising sources for creating indicators on the level of awareness in regards to the protection of children online. However, some efforts are still needed to harmonise the age groups so that minors are captured in these surveys. Other promising sources for data include private sector statistics on sales of parental control data by country as well as statistics on adult-only content on the web as identified for example by search engines.

Table 9. Availability of comparable statistics related to the protection of children online

	Threats	Vulnerabilities	Impact	Prevention	Response
Economic					
Social	H	L	L	L	
Technical	L		H	H	

Note: (H)igh if more than 20% of all discovered indicators are related to a specific field. (L)ow if less than 10% of all discovered indicators are related to a specific field.

CONCLUSION

This report highlighted the potential for the development of better indicators in the areas of information security, privacy, and the protection of children online. It presented areas where there is an underexploited wealth of empirical data that, if mined and made comparable across countries, would enrich the current evidence base for policy making.

The report presented an analytical framework that was used to identify the concentration of existing indicators in specific areas, and most importantly, potential gaps for policy makers. The application of the framework highlighted, for example, that most data sources concentrated on the technical and social aspects, while not covering the economic aspects, which however would be important for policy makers when assessing the socio-economic impacts of potential harms related to security, privacy and the protection of children online.

Based on the analysis presented above, "low-hanging fruit" have been identified, that are areas where better indicators could be developed with minimal resources. They include: *i*) improving the relevance of the OECD model surveys on ICT use by businesses and households/individuals for policy makers in the areas of information security, privacy, and in particular the protection of children online. *ii*) Improving the cross-country comparability of statistics provided by national/government Computer Security Incident Response Teams (CSIRTs) in the area of information security, and privacy enforcement authorities (privacy authorities) in the area of privacy.

The next phase of this project could therefore focus on one of these communities, with the expectation that the development of indicators in other communities covered in this report would build on the experience gained in the first community selected. Irrespective of the community, the next phase of the project would require a deeper understanding of the specific challenges and opportunities related to the selected community. This would for example include analysing internal processes and their impact on the generation of data and statistics as well as the use of standards for the classifications of relevant facts and events.

Such an approach would call for a deeper collaboration with the above mentioned communities but also with policy makers, businesses and the technical community in general. Co-ordination and sharing between all these relevant stakeholders should therefore be encouraged not only to make data collection more efficient but also to allow data sets to be linked.

NOTES

1 The Seoul Declaration "invites the OECD to further the objectives set out in this Declaration […] by […] improving statistical systems to measure the changing access and use of the Internet and related ICT networks by citizens, businesses and institutions in order to provide reliable measures of evolving uses and the impact of the Internet on economic performance and social well-being" (see OECD, 2008).

2 The *Communiqué on principles for Internet Policy-Making* highlights that "the collection, validation and public dissemination of objective data to inform Internet policy decisions should be reinforced and used to augment the combined research capacities of governments, other competent authorities and other stakeholders. International comparable metrics will help to quantify the ongoing economic developments and assess the proportionality and effectiveness of any policy solutions created in multi-stakeholder processes" (see OECD, 2011i).

3 A *honey net* is a network of *honey pots*. A *honey pot* is a system that emulates a set of vulnerable IT services. It is usually "isolated, protected and guarded, but gives the appearance that it contain a vulnerable system of value to the attacker. It thus acts as a fly-papers for malicious code and other attackers" and gives security experts the possibility to analyse attacks and malicious code used live or *ex post* (see http://www.cert.se/honeynet).

4 The term "information security" is used in this report in respect to the mandate of the OECD Working Party on Information Security and Privacy (WPISP) and refers to the "security of information systems and networks".

5 The nature of the risks Internet users are facing is also changing. Malware attacks, for example, are more targeted and no longer limited to the realm of isolated computer hackers, but increasingly originate from organised criminal groups (OECD, 2009; Symantec, 2011).

6 The OECD horizontal project on "New Sources of Growth" is analysing the role of *intangible assets* such as R&D and in particular computerised information (software and databases). This also includes large sets of personal data, which are increasingly providing the foundation for many new business models, in particular, of Internet-based firms. The WPISP together with the Working Party on the Information Economy (WPIE) and the Working Party on Indicators for the Information Society (WPIIS) will jointly work on the analysing the "Economics of Personal Data and Privacy", which will feed the horizontal project on "New Sources of Growth and Intangible Assets".

7 Plewis (2000 cited from Sanderson, 2002), for example, defines evidence-based policies as "policy initiatives [that] are supported by research evidence", and then adds that "policies introduced on a trial basis are to be evaluated in as rigorous a way as possible". In this light, evidence-based policy making has often been compared with evidence-based medicine (EBM). In EBM systematic research are at the core of clinical decisions with the "golden standard" in clinical research being the evidence gathering through randomised controlled trial (RCT), that is the compared treatment with placebos.

8 The last section on the policy makers' needs further elaborates on the use of indicators in particular for supporting the policy making process.

9 The Strategic Policy Making Team of the United Kingdom Cabinet Office (SPMT, 1999) lists the following evidence as example: "Expert knowledge; published research; existing statistics; stakeholder consultations; previous policy evaluations; the Internet; outcomes from consultations; costing of policy options; output from economic and statistical modelling".

10 The WPISP-WPIE Roundtable on "The Economics of Personal Data and Privacy" held in December 2010 also stressed the need for indicators to help understand the economics of personal data.

11 Briefly, an indicator is just a way of saying "how much", "how many", "what size", or "to what extent". For reasons of simplicity, the terms "indicator", "metric", and "statistic" can be used as synonyms.

12 For example, a pilot *Computer Security Survey* conducted by US Census Bureau in 2001 found that information on IT security was generally available but was difficult to collect because of low response rates. The survey had very detailed questions on many aspects of security including *e.g.* on infrastructure, fraud, theft of information, denial of service, sabotage, and viruses, but the results were finally not published because of low response rates (see OECD, 2005b).

13 It should be highlighted, however, that there are other forms of empirical research that fall under the survey umbrella that may not suffer these same drawbacks. For example, surveys involving software that examines security incidents in home computers potentially can get around some of the concerns raised above. In addition, focus groups or experimental research, in which subjects respond to the same stimuli, might avoid problems associated with research that is heavily dependent on recollection.

14 It is important to note that monitoring systems should be privacy-respecting, otherwise the goal of improving privacy would not be achieved overall.

15 The Seoul Declaration "invites the OECD to further the objectives set out in this Declaration […] by […] assessing the application of current OECD instruments addressing […] privacy and security in light of changing technologies, markets and the users behaviour and the growing importance of digital identities [and] improving statistical systems to measure the changing access and use of the Internet and related ICT networks by citizens, businesses and institutions in order to provide reliable measures of evolving uses and the impact of the Internet on economic performance and social well-being".

16 The *Communiqué on principles for Internet Policy-Making* highlights that "the collection, validation and public dissemination of objective data to inform Internet policy decisions should be reinforced and used to augment the combined research capacities of governments, other competent authorities and other stakeholders. International comparable metrics will help to quantify the ongoing economic developments and assess the proportionality and effectiveness of any policy solutions created in multi-stakeholder processes. Data gathering should be undertaken so as to avoid administrative burdens and data analysis should be done carefully to enable sound policy making" (see OECD, 2011i).

17 The OECD (2002) *Guidelines for the Security of Information Systems and Networks* aims among others to "[r]aise awareness about the risk to information systems and networks".

18 The OECD (2003) *Privacy Online: Policy and Practical Guidance* highlights "[p]romoting user education and awareness about online privacy and the means of protecting privacy" as one of its six main elements.

19 Security and privacy indicators on businesses, and households and individuals are provided through the *OECD model survey of ICT use by businesses* and *the OECD model survey of ICT use by households/individuals*.

20 The US National Institute of Standards and Technology (NIST, 2012) Computer Security Incident Handling Guide indentifies three phases it its "incident response life cycle": containment, eradication, and recovery. So questions related to each of these phases could be asked to businesses.

21 The household scope is set to be consistent with that for individuals, so households where all members are outside the age scope will themselves be out of scope (OECD, 2011d).

22 This was the case for CCIRC (Canada), CERT Estonia, CERT-Hungary, GOVCERT.LU (Luxembourg), CERT-MX (Mexico), GovCertUK (United Kingdom), RU-CERT (Russian Federation), and CERT-In (India).

23 See GovCERT.ch (Switzerland)

24 This was the case for the Danish GovCERT, CERTGOVIL (Israel), and Intervention for Computer-related Events (BOME, Turkey).

25 This was the case for Belgium, Czech Republic, Greece, Iceland, Ireland, Italy, New Zealand, Poland, Portugal, Slovak Republic, and Slovenia.

26 See CERT-Bund (Germany) and the US-CERT (United States). CERTA (France) did not publish statistics on alerts and warnings, but statistics could nevertheless be calculated based on data from CERTA's web site.

27 See *www.us-cert.gov/federal/reportingRequirements.html*.

28 To some extent this number can be compared with the number of "intrusion attempts" provided by KRCERT/CC (Korea), although it is unclear if this includes successful and failed attempts.

29 All CERTs reporting incident by sub-categories report the number of DoS attacks, except CERT.at/GovCERT.AT (Austria), KRCERT/CC (Korea) and CNCERT/CC (China).

30 Some CERTs refer to this incident as information break-in, intrusion, invasion, system compromise, hacking incidents.

31 See *www.us-cert.gov/federal/reportingRequirements.html*.

32 For example, CERT.at/GovCERT.AT (Austria) reports the number of "lost credentials", "compromised system", "website defacement" separately. KRCERT/CC (Korea) counts the number of "intrusion attempt" as well as "web defacement". It is unclear, however, whether "intrusion attempt" includes successful as well as failed attempts, making it difficult to compare it with the number of unauthorized accesses.

33 This includes CERT.at/GovCERT.AT (Austria), KRCERT/CC (Korea), GOVCERT.NL (the Netherland), and CNCERT/CC (China).

34 "When this happens, the owners of the stolen identities are usually protected by the operators of the internet services concerned, such as by preventatively changing their password or temporarily deactivating access" (Federal Office for Information Security, 2011).

35 See *www.auscert.org.au/render.html?it=2001*

36 See *www.inteco.es/Seguridad/Observatorio/Estudios/estudio_hogares_4T2010*

37 This includes the Internet Crime Complaint Center, the Council of Better Business Bureaus, the Canadian Anti-Fraud Centre, the US Postal Inspection Service, the Identity Theft Assistance Center, the Xerox Corporation, and the National Fraud Information Center. The following entities have been submitting complaints since 2010: the Canadian Competition Bureau, Catalog Choice, the Center for Democracy and Technology, the Consumer Financial Protection Bureau, the Idaho Attorney General, the Lawyers'

Committee for Civil Rights, the Michigan Attorney General, the Minnesota Department of Public Safety, the Mississippi Attorney General, MoneyGram International, the North Carolina Department of Justice, the Ohio Attorney General, the Oregon Department of Justice, Privacy Star, Publishers Clearing House, the Tennessee Consumer Affairs Division, the Washington Attorney General, and the Western Union Company. (see FTC, 2011).

38 See: *www.ftc.gov/sentinel/*.

39 This data refer to the complaints received no later than calendar year 2006, since "the CSN has a five-year data retention policy; complaints older than five years are purged biannually" (FTC, 2011). Data are broken down by complaint categories, type percentages and count per calendar year. State complaints rates as well as largest metropolitan areas rankings are provided.

40 McAfee has been acquired by Intel Corp. for USD 7.68 billion in 2010.

41 To thwart antimalware programs, malicious users are using *polymorphism*, that is "the ability for malware to dynamically create different forms of itself" (variances) (see Microsoft, 2012). This has made it challenging for antivirus tool providers to identify and count malware as "there can be as many threat variants as infected computers can produce".

42 See *www.cert.se/honeynet.*

43 As described in van Eeten *et al*. (2010), empirical data on botnets typically origin from two types of sources: *i) Data collected external to botnets*. "This data identifies infected machines by their telltale behaviour, such as sending spam or participating in distributed denial of service attacks. And *ii) Data collected internal to botnets.* "Here, infected machines are identified by intercepting communications within the botnet itself, for example by infiltrating the command and control infrastructure through which the infected machines get their instructions".

44 In the case of van Eeten *et al*. (2011), the research project involved combining three big data sets collected through different honey nets: *i*) spam messages, *ii*) Dshield data collected from a global network of sensors run by volunteers; and *iii*) the Conficker Dataset, which is collected by the Conficker Working Group, a working group including IT firms as diverse as Microsoft, Symantec, Verisign, and 1&1.

45 Another promising source of data related to botnets are data collected through anti-botnet initiatives. For example, between September 2010 and November 2011, 1.5 milion users visited the website of the German "AntiBotnet Advisory Center", 340 000 users provided customer information (about infection), and the cleaning tools ("DE-Cleaner") was downloaded 860 000 times.

46 See *http://osvdb.org/.*

47 See *https://ssl.netcraft.com/ssl-sample-report/glossary#certification_authority*

48 See also *https://ssl.netcraft.com/ssl-sample-report/CMatch/certs*

49 This refers to the following question (with the id *i_secpif1*): I have experienced in the last 12 months abuse of personal information sent on the Internet and/or other privacy violations (e.g. abuse of pictures, videos, personal data uploaded on community websites).

50 In many countries, the enforcement authority is a commissioner independent of government; in some others, it is a commission consisting of a body of commissioners, or a group of officials in government departments charged with privacy oversight (OECD, 2006).

51 This is the case, for instance, of the OECD countries which are also members of the European Union, as laid down by article 28.5 of the Directive 95/46/EC.' Ibid.

52 This is also the reason why data on the European Data Protection Supervisor have not been included.

53 Some privacy authorities break down the data on personnel according to the type of contract: *i*) full-time and part-time staff; *ii*) permanent and temporary staff; *iii*) the turnover, personnel on leave, and personnel retiring; the number of staff according to the salary/hierarchical level and external consultant hired.

54 For instance, responding to one query may be worth 0.5, while carrying out an investigation may be worth 40 and writing an opinion may be worth 30 workload points.

55 Tor (The Onion Router) is a system enabling online anonymity.

56 Ghostery is a browser extension for major browsers that enables users to detect and control tracking web components.

57 See *https://www.privacyassociation.org/about_iapp/*

58 See *http://opensecurityfoundation.org/*

59 See metrics.torproject.org/.

60 See www.ghostery.com/faq.

61 Co-operation leads to: producing short courses on privacy/data protection issues to be used by teachers; arranging in concert with the ministry of education the inclusion of privacy/data protection-related contents in school programmes; organising conferences and seminars in schools, or even cine-forums

62 It should be noted at this point, however, that this information is only available in such a way that makes data collection rather difficult.

63 United States v. Xanga.com, Inc., No. 06-CIV-6853 (S.D.N.Y., Sept. 11, 2006) (consent decree).

64 See *www.contentwatch.com/*

65 See *www.cyberpatrol.com/about.asp*

66 See *www.internetsafety.com/*

67 This section is adopted from the OECD (2010d) Consumer Policy Toolkit.

68 It should be noted that the policy making process involves other elements such as for example the consultation with stakeholders, which could take affect at any point in time in the policy making process. The consultation with stakeholders can not only help identify the indicators needed for the policy making process but can also ensure that policy options are expressed clearly and adequately to address all relevant issues. It may also help reveal consequences that are not anticipated or intended by policy makers. This would, for example, be the case when selected policies would interfere with policies in other policy areas, such as competition, consumer protection, and trade, leading to unexpected consequences (see OECD, 2010d).

REFERENCES

Ashford, W. (2011), Information security skills in high demand for 2011, ComputerWeekly.com, 09 August, available at: *www.computerweekly.com/Articles/2011/08/09/247560/Information-security-skills-in-high-demand-for-2011.htm*.

Australian Government, Office of the Privacy Commissioner (2010), "The Operation of the Privacy Act Annual Report 2009/2010".

Banks, G. (2009), "Evidence-based policy making: What is it? How do we get it?", ANU Public Lecture Series, ANZSOG, Canberra, February, available at: *www.pc.gov.au/__data/assets/pdf_file/0003/85836/20090204-evidence-based-policy.pdf*.

Beuth, P. (2011), "Warum Facebook längst nicht alle Daten rausrückt", Zeit Online, 9 November, available at : *www.zeit.de/digital/datenschutz/2011-11/facebook-daten-download*.

CSI (2008), *2008 CSI Computer Crime & Security Survey*, 7 October, available at: *gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf*.

CSI (2010), *2010/2011 Computer Crime and Security Survey*, December, available at: *gocsi.com/survey*.

Davies, P. (2004), "Is Evidence-Based Government Possible?", Jerry Lee Lecture 2004, 4th Annual Campbell Collaboration Colloquium, Washington D.C., 19 February, available at: *www.ebpdn.org/resource/resource.php?id=645*.

European Commission [EC] (808/2004), Regulation No 808/2004 of the European Parliament and of the Council of 21 April 2004 concerning Community statistics on the information society, available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:143:0049:0055:EN:PDF*.

Federal Office for Information Security [Germany] (2011), *The IT Security Situation in Germany 2011*, available at: *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2011_bf_pdf.pdf*.

Federal Trade Commission [FTC, United States] (2011), *Consumer Sentinel Network Data Book for January-December 2011*, February.

Fielder, A., W. Gardner, A. Nairn and J. Pitt (2007), "Fair game? Assessing commercial activity on children's favourite Web sites and online environments". Available at *www.agnesnairn.co.uk/policy_reports/fair_game_final.pdf*.

Gévaudan, C. (2011), "Facebook : la mémoire cachée", Libération.fr, 22 October, available at : *www.ecrans.fr/Facebook-la-memoire-cachee,13424.html*.

GlobalKnowledge (2010), Top 10 Skills in Demand in 2010, available at: *www.globalknowledge.com/training/generic.asp?pageid=2568*

Gomes, L. (2009), "The Hidden Cost of Privacy", Forbes Magazine, 8 June, available at *www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html.*

Hunt, T. (2011), A brief Sony password analysis, Troy Hunt's Blog, available at: www.troyhunt.com/2011/06/brief-sony-password-analysis.html, last time accessed 6.11.2011.

Jaquith, A. (2007), *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, Pearson Education.

Kaemarungsi, K., N. Yoskamtorn, K. Jirawannakool, N. Sanglerdsinlapachai and C. Luangingkasut (2009), "Botnet Statistical Analysis Tool for Limited Resource Computer Emergency Response Team", Fifth International Conference on IT Security Incident Management and IT Forensics, IEEE, DOI 10.1109/IMF.2009.13

Krebs, B. (2011), "Rent-a-Bot Networks Tied to TDSS Botnet", KrebsOnSecurity Blog, September, available at: *krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/, last time accessed: 07.11.2011*

Lubrano, S. (2011), "Digital confidence: bases of trust and impact on usages", January, available at: *findarticles.com/p/articles/mi_hb5864/is_81/ai_n58564012/*

Marston, G. and R. Watts (2003), "Tampering with the Evidence: A Critical Appraisal of Evidence-Based Policy-Making", The Drawing Board: An Australian Review of Public Affairs, 3 (3), March, pp. 143-163, available at: *www.australianreview.net/journal/v3/n3/marston_watts.pdf.*

MessageLabs Intelligence (2010), *2010 Annual Security Report*, available at *www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf*

McAfee (2010), "Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora'", White Paper, available at: *www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.*

McAfee (2011), McAfee Threats Report: Third Quarter 2011, available at *www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf.*

Microsoft (2012), *The evolution of malware and the threat landscape – a 10-year review*, Microsoft Security Intelligence Report: Special Edition, February, available at: *download.microsoft.com/download/1/A/7/1A76A73B-6C5B-41CF-9E8C-33F7709B870F/Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review.pdf*

National Institute of Standards and Technology [NIST] (2012), Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-61, Revision 2, August, available at: *http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf*

Nutley, S., H. Davies and I. Walter (2002), "Evidence Based Policy and Practice: Cross Sector Lessons From the UK", ESRC UK Centre for Evidence Based Policy and Practice, Working Paper 9.

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris, available at *www.oecd.org/internet/interneteconomy/15582260.pdf.*

OECD (2003), *Privacy Online: Policy and Practical Guidance*, in OECD (2009), *Policies for Information Security & Privacy*, OECD, Paris, available at: *www.oecd.org/sti/interneteconomy/49338232.pdf*.

OECD (2005a), "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", OECD Digital Economy Papers, No. 102, OECD Publishing, available at: *www.oecd.org/internet/interneteconomy/35884541.pdf*.

OECD (2005b), "Scoping Study for the Measurement of Trust in the Online Environment", DSTI/ICCP/IIS (2005)1/FINAL, December, available at: *www.oecd.org/sti/interneteconomy/35792806.pdf*.

OECD (2006), *Report on the Cross-border Enforcement of Privacy Laws*, OECD, Paris, available at: www.oecd.org/dataoecd/17/43/37558845.pdf.

OECD (2007), "Measuring Security and Trust in the Online Environment: A View Using Official Data", DSTI/ICCP/IIS (2007)4, January, DOI:10.1787/20716826, available at: www.oecd-ilibrary.org/science-and-technology/measuring-security-and-trust-in-the-online-environment_230551666100.

OECD (2008), *The Seoul Declaration for the Future of the Internet Economy*, OECD Ministerial Meeting of the Future of the Internet Economy, 17-18 June, available at: *www.oecd.org/dataoecd/49/28/40839436.pdf*.

OECD (2010a), "The Evolving Privacy landscape: 30 Years after the OECD Privacy Guidelines", DSTI/ICCP/REG(2010)6/FINAL, 6 April, available at: *www.oecd-ilibrary.org/science-and-technology/the-evolving-privacy-landscape-30-years-after-the-oecd-privacy-guidelines_5kgf09z90c31-en*.

OECD (2010b), "Internet-based Statistics Proposal for a Feasibility Study", DSTI/ICCP/IIS (2010)3, 26 May.

OECD (2010c), *OECD Information Technology Outlook 2010*, OECD, Paris.

OECD (2010d), *Consumer Policy Toolkit*, OECD, Paris.

OECD (2010e), *Efficient E-Government For Smarter Public Service Delivery*, OECD, Paris.

OECD (2011a), "Understanding the Economics of Personal Data: Exploring the Value and Benefits Derived From the Expanding and Innovative Use of Personal Data", DSTI/ICCP/IE/REG (2011)2.

OECD (2011b), "New Sources of Growth: Knowledge-Based Capital Driving Investment and Productivity in the 21st Century", Interim Project Findings, available at: *www.oecd.org/sti/innovationinsciencetechnologyandindustry/50498841.pdf*.

OECD (2011c), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", available at: *www.oecd-ilibrary.org/science-and-technology/cybersecurity-policy-making-at-a-turning-point_5k8zq92vdgtl-en*.

OECD (2011d), *OECD Guide to Measuring the Information Society 2011*, OECD, Paris.

OECD (2011e), *OECD Communications Outlook 2011*, OECD, Paris

OECD (2011f), *Protecting Children Online: Risks Faced by Children Online and Policies to Protect Them*, OECD, Paris

OECD (2011g), "Enhancing Consumer Policy Making: The Role of Consumer Surveys", DSTI/CP(2011)3/FINAL, available at: *http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP%282011%293/FINAL*.

OECD (2011h), "Enhancing Consumer Policy Making: The Role of Consumer Complaints", DSTI/CP(2011)22/FINAL, available at: *http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP%282011%2922/FINAL.*

OECD (2011i), *OECD Council Recommendation Principles for Internet Policy Making*, 13 December, available at: *www.oecd.org/sti/interneteconomy/49258588.pdf.*

OECD (2012a), *OECD Council Recommendation of the Council on the Protection of Children Online*, 16 February, available at: *http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277*.

OECD-APEC (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, OECD, APEC, Paris.

Office of the Irish Data Protection Commissioner (2010), "Twenty-Second Annual Report of the Data Protection. Presented to each of the Houses of the Oireachtas pursuant to section 14 of the, Data Protection Acts 1988 & 2003, PRN. A11/0136"

Plewis, I. (2000), "Educational inequalities and education action zones", in C. Pantazis and D. Gordon (eds.), *Tackling inequalities: Where are we now and what can be done*, Policy Press, Bristol.

Sanderson, I. (2002), "Evaluation, Policy Learning And Evidence-Based Policy Making", Public Administration, 80 (1), pp. 1-22, Blackwell Publishers, Oxford.

Shinder, B. (2010), "Calculating the true cost of cybercrime", TechRepublic, 14 September, available at: http://www.techrepublic.com/blog/security/calculating-the-true-cost-of-cybercrime/4438.

Strategic Policy Making Team of the United Kingdom Cabinet Office [SPMT] (1999), *Professional Policy Making for the Twenty First Century*, Cabinet Office, September, London, available at: www.nationalschool.gov.uk/policyhub/docs/profpolicymaking.pdf

Symantec (2010), "The Silent Epidemic: Cybercrime Strikes More Than Two-Thirds of Internet Users", Press Release, 8 September, available at: www.symantec.com/about/news/release/article.jsp?prid=20100908_01

Symantec (2011), "Symantec Internet Security Threat Report: Trends for 2010", Volume 16, April.

Van Eeten, M., J. M. Bauer, H. Asghari, S. Tabatabaie (2010), "The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis Based on Spam Data", OECD Science, Technology and Industry Working Papers, 2010/5, OECD Publishing.

Van Eeten, M., J. M. Bauer, H. Asghari, S. Tabatabaie (2011), "Internet Service Providers And Botnet Mitigation: A Fact-Finding Study On The Dutch Market", TU Delft, January, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation/tud-isps-and-botnet-mitigation-in-nl-final-public-version-07jan2011.pdf.

ANNEX

Table A.1. National CERTs and supervising administration

Name	Country	Administration	Created
CERT Australia	Australia	Australian Government Attorney-General's Department	Jan-10
GovCERT.AT	Austria	The Federal Chancellery	Apr-08
CCIRC	Canada	Public Safety Canada	Apr-03
Danish GovCERT	Denmark	National IT and Telecom Agency	Jun-06
CERT Estonia	Estonia	Ministry of Economic Affairs and Communications	Jan-06
CERT-FI	Finland	Finnish Communications Regulatory Authority	Jan-02
CERTA	France	French Network and Information Security Agency	Jan-99
CERT-Bund	Germany	Federal Office for Information Security	Sep-01
CERT-Hungary	Hungary	Prime Minister's Office	Jan-05
CERTGOVIL	Israel	Ministry of finance	May-05
NISC	Japan	Cabinet Secretariat	Aug-03
KRCERT/CC	Korea	Korea Internet Security Center (KISC)	Dec-06
GOVCERT.LU	Luxembourg	Prime Minister's Office	Jul-11
CERT-MX	Mexico	Public Security Secretariat	Jun-10
GOVCERT.NL	Netherland	Ministry of Security and Justice	Jun-02
Nor-CERT	Norway	Norwegian National Security Authority	Jan-06
CCN-CERT	Spain	Spanish Ministry of Defence	Jan-07
CERT-SE	Sweden	Swedish Civil Contingencies Agency (MSB)	May-05
GovCERT.ch	Switzerland	MELANI	Apr-08
GovCertUK	United Kingdom	?	Nov-07
US-CERT	United States	Department of Homeland Security (DHS)	Sep-03
RU-CERT	Russian Federation	?	?
CERT.br	Brazil	Brazilian Internet Steering Committee (NIC.br)	Sep-03
CNCERT/CC	China	Ministry of Information Industry	Oct-00
CERT-In	India	Ministry of Communications & Information Technology	Jan-04

Table A.2. Date of establishment of privacy authorities and time span available

OECD Countries	Date of establishment	time-span of the dataset
Australia	1988	2000-2010
Austria	1980	1997-2009
Belgium	1992	2006-2010
Canada	1983	2000-2010
Chile	authority does not exist	
Czech Republic	2000	2000-2010
Denmark	1979	2000-2009
Estonia	1999	2005-2010
Finland	1997	2004-2010
France	1978	1999-2009
Germany	1978	2000-2010
Greece	1997 (law)	2000-2010
Hungary	1995	2000-2010
Iceland	2001	2001-2010
Ireland	1988 (law)	2000-2010
Israel	2006	Data not found
Italy	1996	2000-2010
Japan	2003 (private sector)	Data not found
Korea	KISA: 1996, NIDA 2004	Data not found
Luxembourg	2002	2002-2010
Mexico	2002?	2002-2009
Netherlands	CBP: 1989; OPTA: 1997	2000-2010
New Zeland	1991	2000-2010 (but 2003)
Norway	1980	2000-2010
Poland	1998	2000-2010
Portugal	1994	2000-2010
Slovakia	1998 (law)	2000-2010
Slovenia	1999; 2006 (new body)	2006-2009
Spain	1993	2002-2010
Sweden	1998 (law)	2001-2010
Switzerland	1993	2001-2011
Turkey	?	Data not found
United Kingdom	1984	2009-2011
United States	1914 (FTC)	2000-2010

Table A.3. Link to privacy authorities' annual reports

34 OECD Countries	URL
Australia	*www.privacy.gov.au/materials/types/reports?sortby=29*
Austria	*www.dsk.gv.at/site/6207/default.aspx*
Belgium	
Canada	*www.priv.gc.ca/information/02_05_b_e.cfm#contenttop*
Chile	
Czech Republic	*www.uoou.cz/uoou.aspx?menu=159&lang=en*
Denmark	*www.datatilsynet.dk/publikationer/datatilsynets-aarsberetninger*
Estonia	*www.aki.ee/eng/?part=html&id=96*
Finland	*www.tietosuoja.fi/38071.htm*
France	*www.cnil.fr/en-savoir-plus/rapports-dactivite/*
Germany	*www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TB_node.html*
Greece	*www.dpa.gr/portal/page?_pageid=33,15078&_dad=portal&_schema=PORTAL*
Hungary	*http://abiweb.obh.hu/abi/index201.php?menu=beszamolok*
Iceland	*www.personuvernd.is/utgefid-efni/arsskyrslur*
Ireland	*http://dataprotection.ie/ViewDoc.asp?fn=%2Fdocuments%2Fforms%2FPub%26FormsHome.htm&CatID=5&m=p*
Israel	
Italy	*www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento*
Japan	
Korea	
Luxembourg	*www.cnpd.public.lu/fr/publications/rapports/index.html*
Mexico	*www.ifai.org.mx/Estadisticas/#estadisticas*
Netherlands	*www.cbpweb.nl/Pages/ind_publ_jv.aspx*
New Zeland	*http://privacy.org.nz/corporate-reports/*
Norway	*www.datatilsynet.no/templates/Page____718.aspx*
Poland	*www.giodo.gov.pl/1520113/j/pl*
Portugal	*www.cnpd.pt/*
Slovakia	*www.dataprotection.gov.sk/buxus/generate_page.php?page_id=113*
Slovenia	*www.ip-rs.si/index.php?id=388*
Spain	*www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/index-ides-idphp.php*
Sweden	*http://www2.datainspektionen.se/bt/ladda-ner-a-bestaell?page=shop.browse&category_id=10*
Switzerland	*www.edoeb.admin.ch/dokumentation/00445/00509/01732/index.html?lang=fr*
Turkey	
United Kingdom	*www.ico.gov.uk/about_us/research.aspx*
United States	*http://business.ftc.gov/privacy-and-security*

Table A.4. Example of survey topics by DPA

Country	Topic
Australia	Business, government, community attitudes towards privacy
Canada	Businesses and privacy-related issues, security breaches
Denmark	People's and institutions' privacy awareness
France	Attitudes towards privacy , privacy online, and awareness of the existence of CNIL
Ireland	Public awareness
Israel	Public awareness
Mexico	Public sector's attitude towards access to information
New Zeeland	Public awareness (2006-2008-2010), use of portable devices and international disclosures
Norway	Public awareness, use of data by the police (2004-2010)
Poland	Public awareness and business practices
Slovakia	Public awareness (2005, 2007, 2009)
Spain	Data protection and Security of data in social networks
Sweden	Youth and privacy
United Kingdom	Credit report, business practices, Wi-Fi settings, stakeholder attitudes

Table A.5. Personal data types in DataLossDB

Short Name	Description
CCN	Credit Card Numbers
SSN	Social Security Numbers (or Non-US Equivalent)
NAA	Names
EMA	Email Addresses
MISC	Miscellaneous
MED	Medical
ACC	Account Information
DOB	Date of Birth
FIN	Financial Information
UNK	Unknown
PWD	Passwords
ADD	Addresses

Table A.6. Breach types in DataLossDB

Short Name	Description
Disposal Computer	Discovery of computers not disposed of properly
Disposal Document	Discovery of documents not disposed of properly
Disposal Tape	Discovery of backup tapes not disposed of properly
Disposal Drive	Discovery of disk drives not disposed of properly
Email	Email communication exposed to unintended third party
Fax	Fax communication exposed to unintended third party
Fraud Se	Fraud or scam (usually insider-related), social engineering
Hack	Computer-based intrusion, data not generally publically exposed
Lost Computer	Lost computer (unspecified type in media reports)
Lost Document	Discovery of documents not disposed of properly through loss (not theft)
Lost Drive	Lost data drive, unspecified if IDE, SCSI, thumb drive, etc)
Lost Laptop	Lost laptop (generally specified as a laptop in media reports)
Lost Media	Media (i.e. disks) reported to have been lost by a third party
Lost Mobile	Lost mobile phone or device such as tablets, etc (unspecified in media reports)
Lost Tape	Lost backup tapes
Missing Document	Missing document, unknown or disputed whether lost or stolen
Missing Laptop	Missing laptop, unknown or disputed whether lost or stolen
Missing Media	Missing media, unknown or disputed whether lost or stolen
Snail Mail	Personal information in "snail mail" exposed to unintended third party
Stolen Computer	Stolen desktop (or unspecified computer type in media reports)
Stolen Document	Documents either reported or known to have been stolen by a third party
Stolen Drive	Stolen data drive, unspecified if IDE, SCSI, thumb drive, etc)
Stolen Laptop	Stolen Laptop (generally specified as a laptop in media reports)
Stolen Media	Media (disks or other) generally reported or known to have been stolen by a third party
Stolen Mobile	Stolen mobile phone or device such as tablets, etc
Stolen Tape	Stolen backup tapes
Unknown	Unknown or unreported breach type
Virus	Exposure to personal information via virus or trojan (i.e. keystroke logger, possibly classified as hack)
Web	Computer/web-based intrusion, data typically available to the general public via search engines, public pages, etc.

Source: DataLossDB (http://datalossdb.org)

Table A.7: Initiatives by privacy authorities on the protection of children online

OECD Countries	2000	2010	Type of action
Australia	Y	Y	e-publication
Austria	N	N	
Belgium	N (2007)	Y	websites and debates
Canada	N	Y	websites, school presentations, conference on digital privacy, video contest
Chile			Authority does not exist
Czech Republic	N	Y	competition for children; they have realized a white book of best practices for the protection of children
Denmark	N	Y	magazine for kids
Estonia	N	N	
Finland	N	N	
France	N	Y	website, DPA's Facebook and twitter account
Germany	Y/N	Y	general awareness, no special activity is listed (a code of practice is mentioned, but the translation was not clear)
Greece	N	Y	Dedicated material on the DPA's website
Hungary	n/f	n/f	no data available in the statistics section
Iceland	N	N	
Ireland	N	Y	school programmes, quizzes
Israel	n/f	n/f	Annual Reports not found
Italy	N	Y	Cine-forums, several projects involving high school and university students, artists
Japan	n/f	n/f	Annual Reports not found
Korea	n/f	n/f	Annual Reports not found
Luxembourg	N (2002)	Y	leaflet for young people
Mexico	N (2003)	Y (2009)	conferences for young people
Netherlands	N	N	
New Zealand	N	Y	creation of a youth advisory group formed by high school students which clarified the meaning of privacy for young people and produced targeted material
Norway	N	Y	educational programme ('you decide') and website developed by the University of Oslo
Poland	N	Y	radio programme explaining data protection to young people and competition
Portugal	N	Y	material for teaching in schools, conferences and competition
Slovakia	N	Y	website
Slovenia	N	N	
Spain	Y (2002)	Y	only awareness of the problem, no initiatives mentioned. The privacy of children online: In 2000, they mention a paper on the 'privacy of children online: the role of parental consent in Web browsing', created by the Berlin Group
Sweden	N (2001)	Y	website and information material
Switzerland	N	Y	A toolkit with 10 lessons to be used by teachers and published online
Turkey			Authority does not exist
United Kingdom	(but 2008!)	Y	'I online' project, privacy authorities twitter and Facebook accounts
United States	n/f	n/f	Publication for parents guiding children online, dedicated pages on FTC website