COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.3.2009
SEC(2009) 399

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

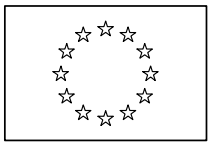
COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on Critical Information Infrastructure Protection
"Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience"

IMPACT ASSESSMENT (Part 3)

{COM(2009) 149}
{SEC(2009) 400}

ANNEX 17: STAFF WORKING PAPER ON THE NATIONAL APPROACHES TO CRITICAL INFRASTRUCTURE PROTECTION IN THE ICT SECTOR



EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

STAFF WORKING PAPER
NATIONAL APPROACHES FOR CRITICAL INFRASTRUCTURE PROTECTION IN THE ICT SECTOR
DRAFT V1.0
3 October 2008

DISCLAIMER
This report does not necessarily represent the views of the Commission

TABLE OF CONTENTS

Contact Person: Alessandra SBORDONI, DG Information Society & Media - INFSO
Tel +32 2 298 45 78, alessandra.SBORDONI@ec.europa.eu

1. INTRODUCTION

This document is a staff working paper prepared by the European Commission as part of the consultation process in preparation of the European policy initiative on Critical Communication and Information Infrastructure Protection – CIIP. This activity is implemented as the Information and Communication Technology (ICT) sector specific approach under the European Programme for Critical Infrastructure Protection (EPCIP) adopted by the Commission in December 2006[1].

The aim of this document is twofold:

1. Record the findings of the stock taking exercise on specific elements of national policies for Critical Infrastructure Protection (CIP) in the ICT sector
2. Serve as a basis for further discussions on the topic. As such, the staff working paper is a living document.

The chapter dedicated to the stock taking exercise provides a detailed synthesis of the responses of Member States (MS) to the second part of the questionnaire on specific elements of national policies for Critical Infrastructure Protection (CIP) in the ICT sector (see the questionnaire in annex). This part of the questionnaire touched upon the following areas:

- Role of information sharing mechanisms
- Role of Public-Private Partnership
- Major challenges on the European and International levels
- The Internet as a Critical Infrastructure (CI) - Contingency plans
- Cross sectors and cross boundaries interdependencies
- Incident response
- The need for and the potential benefit of an EU initiative
- The objectives and scope of an EU initiative
- Mechanisms that may best leverage existing national (and international) activities

[1] See COM(2006) 786 final of 12.12.2006 on a European Programme for Critical Infrastructure Protection at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF and proposal for a directive COM(2006) 787 of 12.12.2006, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:EN:PDF

2. EXECUTIVE SUMMARY

In December 2004, the European Council endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP). As a result of this political decision and further consultations, the Commission decided to put forward a Green Paper on EPCIP[2] outlining the policy options.

On the basis of the replies received and further consultations, the Commission adopted in December 2006, a communication on a European Programme for Critical Infrastructure Protection and a proposal for a directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection[3]. The political agreement between Member States on the directive has been reached in June 2008[4]. Its adoption is expected for the end of 2008.

EPCIP introduced a sector-by-sector approach to CIP at the EU level. The Commission proposal for a directive of December 2006 has identified eleven "critical infrastructure sectors", among which figures Information and Communication Technology (ICT). The Directorate General for Information Society and Media (DG INFSO) is developing the specific approach and measures for the ICT sector.

Under this approach, the Commission plans[5] to develop **a policy framework** to enhance the level of Critical Information Infrastructure Protection (CIIP) **preparedness and response across the EU.** This initiative is expected to build on national and private sector activities related to Critical Infrastructure Protection (CIP) in the ICT sector. It will constitute a significant step forward in the implementation of the Commission strategy for a Secure Information Society defined in COM(2006) 251[6] of 31 May 2006, whose main elements were endorsed by the Council in its Resolution 2007/C 68/01[7].

Consultation of the stakeholders

In view of developing a comprehensive policy framework based on activities already carried out at national level, a stakeholder consultation was launched via a first meeting with Member States' delegates on 05.02.2008.

A questionnaire was sent to Member States to collect inputs and data on specific elements of national policies for Critical Infrastructure Protection (CIP) in the ICT sector including questions dedicated to specific elements of national approaches for the protection of ICT infrastructures. Responses to the questionnaire were received between February and May 2008 from 22 Member States.

---

2 COM(2005)576 final of 17.11.2005, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF

3 Communication: COM(2006) 786 final and proposal for a directive: COM(2006) 787 of 12.12.2006, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:EN:PDF

4 See http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/101001.pdf and the text of the agreed directive at http://register.consilium.europa.eu/pdf/en/08/st09/st09403.en08.pdf

5 Commission Legislative and Work Programme 2008, COM(2007)640 final of 23.10.2007

6 Communication from the Commission on A strategy for a secure Information Society – " Dialogue, partnership and empowerment", COM(2006) 251 final of 31.05.2006.

7 Council Resolution of 22 March 2007 on a Strategy for a secure Information Society in Europe, (2007/C 68/01) of 24.03.2007

A second meeting with Member States' delegates was held on 29.0506.2008. This meeting allowed the presentation of the findings of the stock taking exercise to foster the discussion on topics identified in the stock taking exercise and to gather inputs on the most critical issues that would require further analysis.

A meeting with the private sector stakeholders was held on 26.06.2008 to present the current state of development on EU policies on CIP and CIIP and to gather feedbacks.

Further meetings with Member States' delegates possibly in conjunction with the private sector might be scheduled in the second half of 2008 and in the beginning of 2009.

* * *

SUMMARY OF THE RESPONSES TO THE SECOND PART OF THE QUESTIONNAIRE

The role of information sharing mechanisms

There is general agreement among the respondent Member States that information sharing mechanism at European and International level is useful, however establishing trusted point of contacts is considered as a priority.

Information sharing is generally viewed as a very useful tool to foster preparedness regarding resilience and protection of CI.

The focus of information sharing should be on best practices, new threats, risk management, mutual help.

The scope of information sharing should be limited to a consultative framework for CIIP at EU level and a bottom-up approach should be followed before adopting regulatory measures.

The role of public private partnerships

PPP at national level play a very important role in almost all MS that responded, whereas some MS have not yet defined in their national strategy what the role of PPP is.

Only one MS does not support the idea of PPP at EU level and another one does not favourably consider a formalised PPP at EU level advocating a somewhat looser form of PPP.

There is anyway general agreement from respondent Member States that PPP at EU level would play an important role.

It has been pointed out that PPP at EU level is desirable, but difficult to implement because it is too much dependent on the good will of different actors. To solve this problem it has been suggested to promote PPP in certain specific areas where a considerable number of stakeholders are interested (e.g. banks, major ISPs)

It has also been stressed that it is important to attribute roles and responsibility to the relevant stakeholders and the public sector, taking into account that fostering preparedness and enhancing the level of global protection is a responsibility that lies with the public sector and has not to be shifted to the private sector.

Potential focus at EU level would be on promotion of best practices, expert support (cooperation among CERTs; workshops between Government and private sector) and implementation of measures to protect CI.

Major challenges for critical infrastructures in the ICT sector on EU and International levels

Some respondent Member States have not yet developed a national policy on the protection of Critical Infrastructures in the ICT sector.

Major challenges mentioned:

- All hazard risk preparedness
- Enhancing activities for the prevention of large scale attacks
- Improve ICT cooperation, agreements and regulation in ICT sector
- Interdependencies between national CI e.g. cross-border networks and the identification of which NCI are characterised by cross-border dependencies
- Distortion of fair competition
- Over-regulation, role of EU and international bodies, respect of subsidiarity principle
- Issue of deficit of domestic control

Internet as a critical infrastructure

Almost all the responding MS consider Internet as a CI or part of CI.

Internet is regarded as a CI in a different way when compared to other sectors such as energy and transport. Internet is considered as a critical infrastructure with regard to the provision of services, e.g. connectivity to end-users and maintenance of connection to the rest of the world.

In general, contingency plans are/will be implemented by the private sector and overall contingency plans at national level do not exist yet. One MS pointed out that a specific contingency plan is under development.

An area of EU and international activity could be the exchange of best practices for the design of such contingency plans and to ensure a high robustness of the Internet infrastructure.

Cross sectors and cross boundaries interdependencies

Cross-border and cross-sector interdependencies are widely recognised as a key issue by almost all responding MS. However, a specific approach to identify and analyse the relevant domestic implication has not yet been developed in some respondent MS that have not yet specifically addressed these issues.

Many respondent Member States consider important to identify the interdependencies between services both domestically and outside national borders and provided some examples of their national approach.

- Specific Working Groups formed by companies operating in different sectors develop guidelines and contingency plans.

- Definitions and approaches of the national strategy take into account the interdependencies between critical infrastructures for the ICT sector and for other sectors like food, water, health, transport and energy.

- The analysis of interdependencies between services inside and outside national borders is taken into account as the services for critical infrastructure depend on many CII components, also of cross-border nature.

With regard to the issue of cross-border interdependencies, almost all respondent Member States expressed their favourable opinion towards cooperative work in this area at European level.

In particular, it was stressed that an EU activity regarding the protection of the ICT infrastructures could support efforts in analysing cross border issues.

Incident response

In almost all responding Member States, from a technical perspective, emergency response is managed by dedicated facilities such as CERTs. However, generally speaking incident response does not fall within the responsibility of one single national authority or body and it is mostly based on a general approach and not on a sector specific approach.

Some contributors made no specific reference to CIIP policy and did not mention governmental/national CERTs.

It has to be noted that the private sector was mentioned as one of the key actors and PPP are encouraged in order to better organise effective counter measures and minimise the impact of incidents.

The need for and the potential benefit of an EU initiative

The contributors showed general support to an EU initiative on CIIP and suggested to focus on:

- Criteria and best practices

- Minimal requirement for a European approach to CIIP

- Analysis of international dependencies

- Setting up an expert group on CII

- Harmonisation of sectoral criteria
- Bottom up approach
- Industry consultation and workshops, engaging ENISA.

3. STOCK TAKING

This chapter provides an overview of how Member States deal with specific elements of the protection of Critical Infrastructure in the ICT sector. It is based on the written responses to the questionnaire – Part 2 in annex.

Question 1: What is the role of information sharing mechanisms to foster preparedness concerning resilience and protection of national critical infrastructures in the ICT sector (and, in particular, for CII)?

- *Does your government consider information sharing on the European and International levels to be a need and/or a priority? If yes, what might be the focus and scope of such an activity?*

Information sharing is generally viewed by most contributors as a useful tool to foster preparedness regarding resilience and protection of critical infrastructure (CI) both at national and at EU levels.

One contributor pointed out that the protection of important information systems and critical information infrastructures is an integral part of the National Security Strategy. In particular, concerning critical information infrastructures (CII), key ICT providers participate in a forum where companies provide information about outages, failures, and major incidents that have occurred to their infrastructures. In times of crisis all governmental decisions, requests and information gathering is conducted through this system; the government CERT is also connected to this system, thus enabling the infrastructure of the participating companies to be more resilient in case of a cyber attack or incident.

Another contributor mentioned that information sharing at national level is addressed by the national Act on Crisis Management, which provides for a national early warning system and a national alert system.

The role of NRA

Some contributors indicated that at national level the National Regulatory Authority for electronic communication (NRA) plays an important role as a centre for information sharing among relevant stakeholders. In particular:

- the NRA has set up dedicated fora where public and private organisations' contact points share information regarding network and information security issues;

- the NRA leads the process of issuing technical regulations for public communication networks and services involving relevant stakeholders, in order to better focus on resilience and protection of those network and services;

- the NRA formally shares information in existing governmental mechanisms and have extensive bilateral information sharing with relevant agencies;

- the NRA is part of a group (Electronic Communication – Resilience and Response Group) formed by all the major telecom providers and relevant government departments responsible for information sharing regarding best practices on network

resilience. This forum is the focal point for the industry in case a coordinated response is required during an emergency.

The role of information sharing at EU level

Most contributors agree that information sharing mechanisms at European and International level are very useful taking into account that networks and ICT security are cross boundary in nature.

Among these, some contributors mentioned that information sharing at EU level is desirable but, due to the sensitivity of the matters, it is of primary importance to establish mutual trusted relationships between the private sector and the government at national level first before information sharing mechanisms can be expanded at EU level.

In particular one contributor mentioned that information sharing regarding threats in the ICT sector is essential for what concern the technical perspective and has proved successful between dedicated technical facilities. Information sharing has proved especially successful between national CERTs, e.g. the Forum of Incident Response and Security Teams (FIRST) or the European Government CERT (EGC) Group. At a specific EU level, the ENISA working group *CERT co-operation and support* and the feasibility study for a European Information Sharing and Alert System EISAS are considered useful elements to foster preparedness concerning resilience and protection of CII. Another contributor stressed that information sharing is an important tool for preventing incidents, early warning, detection and reaction to incidents and it is considered crucial in every phase of building resilience and protection of CI. This contributor also mentioned that, while there is efficient cooperation at European level for what concerns the operational level (e.g. between CERTs, law enforcement structures, intelligence agencies, etc.), information sharing is almost absent at policy making level where different countries consult each other very rarely.

Scope and focus of information sharing at EU level

Regarding to the scope of information sharing at EU level, it was suggested:

- to set up a consultative framework for CIIP at EU level;
- to limit the scope of information sharing to situations where cross-border interdependencies exist;
- to follow a bottom-up approach before adopting regulatory measures at EU level;
- information sharing at EU level should be limited due to the sensitivity of the matter involved (e.g. not covering ECI location under the control of a single national Government);

For what concerns the focus of information sharing at EU level most contributors pointed out that it should be on best practices, new threats, risk management and mutual help.

Question 2: What is the role of public private partnerships to foster preparedness and enhance the level of protection of national critical infrastructures in the ICT sector (and, in particular, for CII)?

Public Private Partnerships (PPP) at national level play an important role in almost all MS that responded. The involvement of the private sector to foster preparedness is considered essential given the fact that many ICT critical infrastructures are owned by private companies due to the liberalization process.

One contributor pointed out that its national cyber defence is greatly based on PPP which have developed into an efficient network and have created a favourable environment among all parties involved. PPP at international level is considered desirable but difficult to implement because it mostly depends on the good will of private sector actors to cooperate. In order to solve this problem at national level, these partnerships have been launched in certain specific areas where a considerable number of stakeholders are interested (e.g. financial institutions as well as major ISPs have been interested and very active in participating in joint activities).

Some contributors provided examples of PPP at national level:

- the Ministry in charge of Informatics and Communication contracted a Foundation to operate the national CERT. In addition, a project was launched to provide the general public with a website containing information on IT security issues such as spam, viruses, and other threats and on the possibilities to protect privacy in an easy understandable manner;

- Both the national CERT and the National Centre for information security are PPP.

- A National Crisis Management Co-ordination group has been set up. The group works on a voluntary basis where members from major telecommunications providers and the NRA work regularly on a bilateral level on how to establish robust electronic communication.

Some contributors mentioned that the role of PPP has not been defined yet in their national strategy.

- *Does your government consider public private partnership on the European and International levels to be a need and/or a priority? If yes, what might be the focus and scope of such an activity?*

Several contributors agree that PPP at EU level is a need and a priority whereas one Member State has not yet considered the need of PPP at EU and international level.

Another respondent does not favourably consider a formalised PPP at EU level, advocating instead a somewhat looser form of PPP. In particular, this contributor pointed out that there is scope for partnerships on an international level that would complement the work carried out by Member States at national level on their internal communication infrastructures.

Among the contributors which support PPP at EU level and considered it as a need, one contributor stressed that it is very important to attribute roles and responsibility to the relevant stakeholders, bearing in mind that fostering preparedness and enhancing the

global level of protection is a responsibility that lies with the public sector and has not to be shifted to the private sector.

For what concern the potential focus at EU level, contributors mentioned the promotion of best practices, expert support e.g. cooperation among CERTs, workshops between Government and private sector, and implementation of cross-border measures to protect CI.

Question 3: What does your government consider to be the major challenges for preparedness, resilience and protection of critical infrastructures in the ICT sector (in particular, for CII) on the European and International levels?

- *How are those challenges addressed in your national policy?*

Some contributors pointed out that a specific national policy on the protection of Critical Infrastructures in the ICT sector has not been developed yet.

Among those Member States who have a national strategy in place, the following major challenges were identified:

- All hazard risk preparedness approach which takes into account the interdependencies between critical infrastructures in different sectors. In particular, the basic principles of the national policy are subsidiarity, synergy and complementarity, as well as proportionality and confidentiality.

- Prevention of large scale attacks and the promotion and implementation of related activities. In this context, it was pointed out that the only international legal instrument on cyber security is the Council of Europe Convention on Cyber crime. Therefore the idea of developing new international legal instruments on CIIP could be considered as a useful mechanism to prevent the attacks on CII. In addition to multilateral regulatory efforts, it is considered vital to promote a culture of cyber security and raise awareness on cyber threats and educate the population on information security and on responsible use of Internet especially. At the operational level, the international crises management exercises that involve also recovery plans are very important.

- Culture of resilience and security. It was pointed out that there is an endemic challenge to ensure that the importance of resilience and security is ingrained within the business culture of communications companies. There is also a need to get the right balance between legislation/regulation on security and resilience on the one hand, and consensual partnership approaches to encouraging security and resilience on the other. The national government broadly favours the encouragement and the use of standards to gain acceptance of operators: a proposal to introduce a minimum standard for the telecommunications industry as a whole for interconnections and shared facilities has been put forward; this might allow e-communications providers to be able to exceed this standard and therefore differentiate themselves in the market.

- Interconnection between national infrastructures. It is considered very important to identify the critical infrastructures with cross-borders dependencies. Early warning

mechanisms at European level, along the lines of what is already in place at the national level, need also to be considered as a major challenge.

- The potential distortion of fair competition. They considered that legal obligations at EU or national level for private operator to enhance the level of security of their networks could hamper the promotion of competition at international level between companies that incur extra costs related to security requirements and companies that are still allowed to cut security related costs and offer lower prices.

- The risk of over-regulation in the ICT sector: the role of EU and international bodies has to be clarified and the principle of subsidiarity has to be respected.

- The issue of deficit of domestic controllability, a situation where part of the CI could belong or be controlled by an un-trusted foreign party (e.g. a "silent" acquisition of an ISP by some unknown company based in an un-trusted country, while the ISP provides critical services within the national territory). However, no policy has been approved yet on what action the government should take if a CI provider is acquired by an un-trusted foreign party.

- Along the same line, another contributor stressed the importance of raising awareness of the role played by each single country for the security of critical infrastructures belonging to other countries. A specific Working Group on CIIP is addressing these challenges.

Question 4: Does your government consider the Internet as a critical infrastructure? If yes, what are the policy initiatives to address this aspect?

- *Do contingency plans exist for the Internet-related failure in your country? What are their main objectives and scope?*

- *Does your government consider desirable that such contingency plans (and related exercises) would exist in most countries? Is there any scope for a European and/or International work in this area?*

Most responding MS , taking into account its cross-border nature and the convergence of the different telecommunication and data networks, consider Internet as a CI or as part of CI.

It has to be noted, however, that the Internet is considered a CI in a different way when compared to transport and energy sectors: Internet is considered as a CI with regard to the provision of services (e.g. connectivity to end-users and maintenance of connection to the rest of the world). What is important is to stress the difference between the technological infrastructures of the Internet formed by many networks and many redundant components self-supporting to a large extent, and the criticality of the services and functions provided through the Internet. Another contributor stressed that the underlying services and applications of the Internet – not the Internet as such – can be considered as CI.

National initiatives

With regard to the national initiatives which address the criticality of the Internet infrastructure four major strategies with different scope were mentioned:

- A Cyber Security Strategy whose main objective is to guarantee the operation of the critical e-services for citizen and organisations and to minimise the disruptions of the Internet. In this respect, it was pointed out that specific measures to strengthen the Internet infrastructure are planned to be introduced together with new regulations for the e-Communication sector.

- The protection of the Internet and CII is addressed in the national Strategy for securing Vital Function to Society. In addition, other tools are in place to further develop CIIP, including legislation which provides mandatory requirements for operators to implement contingency plans.

- A national strategy to secure the Internet was proposed by the NRA at the request of the Government. The strategy includes an action plan, a designation of responsibility, and a management plan. The aim of the strategy is to facilitate and clarify future work to secure the infrastructure of the Internet and is directed at those parts of the infrastructure that are unique to the Internet.

- Another contributor underlined that, given the increasing importance of Internet services such as e-commerce, e-business and e-government and the raising dependence on e-mail and web communication, the ICT operators have been integrated in the working groups established in the context of the national CIP implementation Plan. The task of these working groups is to carry out common exercises, to define common scenarios and to establish a contact database for implementing early warning mechanisms.

Contingency plans

In general, contingency plans are implemented by the private sector in order to cope with the possibility of non-availability of certain parts of the Internet.

According to all the responding contributors, overall contingency plans at national level have not been developed yet.

In particular, it was mentioned that there are no official harmonised country-wide contingency plans for Internet-related failures, although such plans exist for all major operators of telecommunication infrastructure on an individual basis. The main objectives of existing contingency plans are stability and high availability by means of redundancy and fault-tolerant solutions, e.g. highly distributed systems like anycast or mirrored sites for Internet Exchange Points. It was mentioned however that a specific contingency plan is under development in one MS.

Several contributors considered that the implementation of such contingency plans in most countries would be desirable due to the inherently international nature of the Internet, in particular to ensure that the international Internet backbone and central services like DNS are highly available.

One contributor mentioned that an area of EU and international work could be exchange of best practice for the design of such contingency plans and to ensure high robustness of the Internet infrastructure.

Question 5: How does your government assess and address the cross sectors and cross boundaries interdependencies of critical infrastructures for the ICT sector?

- *How is the issue of potential exposure of National critical infrastructures for the ICT sector to interdependencies with infrastructures in other sectors outside the national borders addressed? Is this an area for possible European and/or International work?*

Some contributors) pointed out that the issue of interdependencies, both cross-sector and cross-borders, is not yet addressed in their national policies. Nevertheless the importance of cross-sector and cross-border interdependencies is widely recognised but a specific approach to identify and analyse the relevant domestic implication has not yet been developed.

Many respondent Member States consider important to identify the interdependencies between services both domestically and outside national borders.

Examples of National approaches

- One national approach is based on the work of specific Working Groups where companies providing services in different sectors are participating to develop guidelines and contingency plans taking into account cross-sectors aspects and related risks.

- It was mentioned that the definitions and approaches of the national strategy take into account the interdependencies between critical infrastructures for the ICT sector and for other sectors like food, water, health, transport and energy. Along the same line it was mentioned that the analysis of interdependencies between services inside and outside national borders is taken into account as the services for critical infrastructure depend on many CII components, also of cross-border nature.

- It was also stressed that interdependencies are addressed in the national strategy to secure the Internet, and, along the same line, another contributor pointed out that the analysis of these interdependencies is a priority in the context of the activities for the implementation of the national policy for CIIP. However, cross-border issues regarding the ICT sector have not yet been addressed in a structured way as it has been done for other sectors such as the energy one.

- It was mentioned that cross-sector interdependencies are addressed under the activities of the National Security on Critical Infrastructure Protection where the analysis of dependencies on the ICT-sector and -subsectors are prioritized. However, cross-border issues regarding the ICT sector have not yet been addressed in a structured way whereas for what concerns the energy sector these issues have been discussed bilaterally or in the framework of international organizations and have lead to guidelines or agreements.

Cross-border interdependencies

With regard to the issue of cross-border interdependencies, almost all respondent Member States expressed their favourable opinion towards cooperative work in this area at European level.

In particular, it was stressed that an EU activity regarding the protection of the ICT infrastructures could support efforts in analysing cross border issues. This is considered very important given the fact that many private parties providing public telecom infrastructure and/or services are operating internationally throughout the EU.

Question 6: How is incident response organised in your country? What are the national incident response capabilities and how do they work/cooperate together?

- *What is the role of government? What is the role of the private sector?*

In almost all responding Member States, from a technical perspective emergency response is managed by dedicated facilities such as CERTs. However, generally speaking incident response does not fall within the responsibility of one single national authority or body and it is mostly based on a general approach and not on a sector specific approach.

Some contributors made no specific reference to CIIP policy and did not mention governmental/national CERTs.

It has to be noted that the private sector is one of the key actors and PPP are encouraged in order to better organise effective counter measures and minimise the impact of incidents.

The respective roles of the Government and the private sector with regard to incident response capabilities

One contributor mentioned that a governmental crisis coordination centre, not only dedicated to the ICT sector, operates a 24/7 early warning function to inform and assist the relevant governmental bodies in time of national crisis.

Along the same line, another contributor mentioned that protection from national disasters is regulated under the Crisis Management Act which describes the roles and responsibility of the main national bodies involved in the management of the units of the Integrated Rescue System. In particular, for what concerns the role of the Government it is the Ministry of State Policy for Disasters and Accidents that, in cooperation with the relevant institution, carries out the civil protection activities, organizing and developing methodologies for risk assessment in case of disaster. With regard the role of the private sector, the companies which operate with hazardous substances, potentially dangerous for the population and the environment, have to prepare their own teams for rescue activities, take preventive measures and prepare security plans.

One contributor mentioned that incident response does not fall under the responsibility of one single national body. For what concerns the ICT structure of governmental bodies, a specific Centre was made operational on recently within the framework of the central

agency responsible for prevention, monitoring, handling, data collection and incidents analysis. Incident response is complemented by cyber crime prevention and repression by law enforcement authorities. In particular, the role played by the Government is to promote new forms of cooperation with the private sector to handle all incidents, in light of existing regulations and good practices.

Another contributor mentioned that the Government has created an operational centre for information systems security, whose mission is to ensure the coordination of ministries in preventing and protecting themselves from cyber attacks. It was also mentioned that in general it is the responsibility of the private sector to pursue activities to enhance the resilience of the systems, including recovery planning and other preparedness activities, although the national government coordinates activities to ensure immediate crisis response.

Another contributor provided a detailed description of the role of the different governmental bodies involved in crisis management at national, regional and local level. In particular, the central government plays a key role in the organisation of national defence strategies coordinating activities of the different ministries in charge for the relevant sectors. For what specifically concerns CIIP policy, the relevant tasks are mainly allocated within the Ministry of Economic and Transport which coordinates the various activities for the maintenance and development of the national economic infrastructure.

One respondent Member State mentioned that at national level it is the Civil Protection Department which is responsible for incident response.

Another contributor described that incident response capabilities are distributed over a number of national agencies. In the ICT sector, the NRA facilitates and chairs the National Telecommunications Coordination Group whose mission is to support the restoration of national infrastructures of electronic communications during critical disturbances.

Along the same line another contributor pointed out that the government has a coordinating role, bringing together critical infrastructure owners to work on reducing vulnerabilities, whereas the private sector has the expertise to develop and propose the necessary steps to reduce vulnerabilities.

Another contributor mentioned that, in general, the private sector is responsible for restoring service to their customers during an emergency situation. However, in some situations where the scale or complexity of an emergency is such that some degree of government co-ordination or support becomes necessary, a designated Lead Government Department or, where appropriate, a given administration, is responsible for the overall management of the government response. The Government maintains dedicated crisis management facilities and supporting arrangements which are only activated in the event of a major national emergency and has the power to direct the companies to undertake actions for the common good in an emergency situation.

Question 7: What does your government consider to be the need for and the potential benefit of an EU initiative to enhance the level of preparedness and response for the protection of critical infrastructures in the ICT sector (and, in particular, for CII)?

- *What might be the objectives and scope of an EU initiative to add value to the policies and activities in your country and internationally? What might be the focus and priorities of such an EU initiative?*

- *What mechanisms may best leverage existing national (and international) activities?*

All contributors showed general support to a potential EU initiative in the area of CIIP.

In particular, one contributor mentioned that it could be useful if within the EU minimal requirements for CIIP in the ICT sector would be established. The EU could adopt one of the existing frameworks for CIIP or develop a new one that suits the needs of most EU countries. In this respect the commonly agreed principles on cooperation between the member states could be useful for cross-border CII and services protection. It would also be useful at EU level to launch awareness campaigns or to promote awareness via national authorities.

Another contributor stressed that the main need would be to create a communication infrastructure with a shared protocol to facilitate the exchange of information and warning messages among the national bodies (or agencies) involved in the incident response handling and that one of the objectives of an EU initiative should be the enhancement of awareness level in this sensitive matter.

Other suggested approaches included:

- Harmonisation of sectoral criteria and sharing of best practices
- Analysis of international dependencies conducted at EU level
- Setting up an expert group on CII,
- Bottom up approach
- Industry consultation and workshops, engaging ENISA

ANNEX

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 1 February 2008

QUESTIONNAIRE

ON SPECIFIC ELEMENTS OF NATIONAL POLICIES FOR CRITICAL INFRASTRUCTURE PROTECTION IN THE ICT SECTOR

In the legislative work programme for 2008 [COM(2007) 640], the Commission announced a policy initiative on critical communication and information infrastructure protection (CIIP). An important element of this initiative will be the process to define the criteria to identify the European Critical infrastructures for the ICT sector as foreseen by the current Commission's proposal on a European Programme on Critical Infrastructure Protection.

In preparation of this initiative and as a part of the consultation process, the Commission services have developed the present questionnaire to gather information from Member States on specific elements of their National policies for critical infrastructure protection for the ICT sector.

The questionnaire is composed of two parts. Part 1 focuses on the criteria for identification of critical infrastructures in the ICT sector. Part 2 covers other policy aspects. Sub-questions, identified by the italic formatting, aim to further guide respondents in the related area.

Answers to this questionnaire should be sent by **15 March 2008** to:

Mrs Alessandra Sbordoni,

DG Information Society and Media,

Unit A3 - Internet; Network and Information Security

E-mail: Alessandra.SBORDONI@ec.europa.eu

CRITERIA

a) Which definition is used, in your country, for critical infrastructures in the ICT sector (and in particular for critical communication and information infrastructures)?

   - *Is the notion of "critical communication and information infrastructure" (CII) used? If yes, what does it refer to?*

   - *How are definitions important to get stakeholders involved in and committed to initiatives/activities on protection of critical infrastructures in the ICT sector?*

b) Which steps and criteria are used in your country to identify and designate National critical infrastructures in the ICT sector (and, in particular, for critical communication and information infrastructures)?

   - *Is the private sector involved in identifying and designating national critical Infrastructures in the ICT sector? If yes, how?*

   - *Are risk-based management approaches used? If yes, which ones? What are the main processes involved in those approaches? What are the respective roles of the government and the private sector?*

c) How do existing definitions and approaches to identify and designate national critical infrastructures in the ICT sector apply for cross-border and international critical infrastructures in the ICT sector?

   - *What is the approach taken to define and identify trans-border resources and/or infrastructures critical for your country?*

POLICY ASPECTS

d) What is the role of information sharing mechanisms to foster preparedness concerning resilience and protection of national critical infrastructures in the ICT sector (and, in particular, for CII)?

   - *Does your government consider information sharing on the European and International levels to be a need and/or a priority? If yes, what might be the focus and scope of such an activity?*

e) What is the role of public private partnerships to foster preparedness and enhance the level of protection of national critical infrastructures in the ICT sector (and, in particular, for CII)?

   - *Does your government consider public private partnership on the European and International levels to be a need and/or a priority? If yes, what might be the focus and scope of such an activity?*

f) What does your government consider to be the major challenges for preparedness, resilience and protection of critical infrastructures in the ICT sector (in particular, for CII) on the European and International levels?

   - *How are those challenges addressed in your national policy?*

g) Does your government consider the Internet as a critical infrastructure? If yes, what are the policy initiatives to address this aspect?

   - *Do contingency plans exist for the Internet-related failure in your country? What are their main objectives and scope?*

- *Does your government consider desirable that such contingency plans (and related exercises) would exist in most countries? Is there any scope for a European and/or International work in this area?*

h) How does your government assess and address the cross sectors and cross boundaries interdependencies of critical infrastructures for the ICT sector?

- *How is the issue of potential exposure of National critical infrastructures for the ICT sector to interdependencies with infrastructures in other sectors outside the national borders addressed? Is this an area for possible European and/or International work?*

i) How is incident response organised in your country? What are the national incident response capabilities and how do they work/cooperate together?

- *What is the role of government? What is the role of the private sector?*

- *What are the mechanisms and arrangements in place for cross border cooperation on incident response?*

j) What does your government consider to be the need for and the potential benefit of an EU initiative to enhance the level of preparedness and response for the protection of critical infrastructures in the ICT sector (and, in particular, for CII)?

- *What might be the objectives and scope of an EU initiative to add value to the policies and activities in your country and internationally? What might be the focus and priorities of such an EU initiative?*

- *What mechanisms may best leverage existing national (and international) activities?*

ANNEX 18: FLASH REPORTS

ANNEX 18 A: CYBER ATTACKS TARGETING LITHUANIAN WEBSITES

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 04 July 2008

FLASH REPORT

CYBER ATTACKS TARGETING LITHUANIAN WEBSITES

1. WHAT HAPPENED?

- Press reports dated from June 30th suggest that recently accepted legislation in Lithuania banning communist symbols across Lithuania, has prompted http://blogs.zdnet.com/security/images/lenin_statue_at_grutas_park.jpghackers to start defacing Lithuanian web sites.

- These press reports also suggest that an indication of the upcoming attacks was detected last week with active discussions on Russian-speaking on-line forums.

- According to Sigitas Jurkevicius, a computer specialist at Lithuania's communications authority: "More than 300 private and official sites were attacked from so-called proxy servers located in territories east of Lithuania. The hackers hit Web sites from both the government and private sector". Of possible interest and significance is the fact that pretty much all of the 300 defaced web sites were hosted on the same ISP, Hostex, previously known as Microlink. This may indicate the existence of a common vulnerability that facilitated these attacks.

- The zdnet.com report suggests that "so far, the volume of discussion and collaboration in this attack isn't indicating upcoming DDoS attacks, in the sense of distributing tools and lists of vulnerable sites, sites to be attacked, and compromised hosts to execute the attacks from, as we've seen it happen in Estonia's incident."

2. ASSESSMENT AND ANALYSIS:

- The primary aspects of the incidents in Lithuania are **matters of Lithuanian national sovereignty,** where it will be for the Lithuanian government to decide what action to take and what support they would like to receive from international partners and institutions such as the EU.

- The incident *may* look similar to the cyber attacks targeting Estonia last year but early indications are that it has a different profile with defacement of web-sites being the main purpose of the attacks rather than widespread "denial of service". It is unclear that the attack is still ongoing.

3. LINE TO TAKE:

- The Commission is aware of the current events in Lithuania which appear to represent a large-scale cyber attack from persons as yet unknown.

- There is of course a heightened awareness of this type of event following the attacks on Estonia last year.

- The issue is primarily a matter of national sovereignty and may well prove to be a matter of national security as well, so it would not be appropriate for the Commission to comment further in any detail in public at this point in time.

- That said, because of the global nature of the Internet, "no man is an island" and each country, inevitably, has a degree of inter-dependence on other countries, not least when it comes to responding these types of attacks.

- Furthermore, these attacks are additional evidence of the need for a European Union incident response capability. Such capability would help to reinforce the initiatives which are already implemented at national level. This is something that the Commission is already seeking to facilitate as part of the ongoing critical infrastructure protection initiatives at EU level. To this end, the Commission intends to make proposals to the Member States at the beginning of 2009, taking full account of the important role and responsibility that will need to be taken by the private sector.

DEFENSIVE POINTS:

Question: what is the Commission doing to protect critical information infrastructures?

- The Commission is actively engaged in developing a European programme for critical communications and information infrastructure protection. This work is carried out within the broader context of the European programme on Critical infrastructure protection.

- Discussions related to Internet security took place in a workshops, at the initiative of the European Commission, on lessons learnt from large scale attacks on the Internet on 17.01.08. The participants underlined that Internet security and stability is a **shared responsibility.** They stressed the fundamental necessity to build further the resilience and robustness of the Internet; **response preparedness is equally crucial**. More cooperation, information and best practice sharing as well as partnership between public and private stakeholders, across sectors and geographical boundaries are needed.

- One of the areas of action of the future CIIP initiative is to strengthen incident response capability for Europe building on existing national capabilities and initiatives. The intention is to invite Member States to establish/reinforce national incident response capability as a key resource for preparedness, information sharing, coordination and incident response.

4. PUBLICLY AVAILABLE PRESS REPORTS:

Sources:
http://ap.google.com/article/ALeqM5gqkayLOYlkT2S8HI6B_tb18xls9wD91KGLH80
http://www.alfa.lt/straipsnis/c78573
Some info (and screenshots of the defacement) from local LT websites:
http://www.informacijosapsauga.lt/blogietis/rusijos-hakeriai-ateina/
A partial list of affected website is reported here, scroll down (list not verified, they are reports from LT users):

http://www.geradiena.lt/Balius-tesiasi-Kiti-nulauzti-tinklalapiai_457
Among which are:
http://www.vtek.lt
http://www.baltijos.lt
http://www.unicef.lt/
http://www.mitsubishi-motors.lt/
http://www.a1auto.lt/
http://www.mokykla.lt/
http://www.a1auto.lt/
http://www.jbblegal.lt/
http://www.komaa.lt/

ANNEX 18 B: CYBER ATTACKS TARGETING GEORGIAN GOVERNMENT WEBSITES

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 21 August 2008

FLASH REPORT

CYBER ATTACKS TARGETING GEORGIAN GOVERNMENT WEB-SITES

1. WHAT HAPPENED?

- According to press reports in various on-line sources such as *Tagesschau*, *CNET* and *The Register* dated mid August, **web-sites in Georgia have been targeted by attacks such as distributed denial of service (DDoS) and defacing/ hijacking**. The attacks appear to coincide with recent events involving Russia and Georgia. According to some observers the attacks started on 8 August hitting the South Ossetian government web-site and peeked until 13 August; whether they are ongoing is not clear. Affected web-sites appear to have included those belonging to the South Ossetian radio station, Georgian press agency 'Civil', Georgian presidential and other government web-sites. The presidential web-site is reported to have been targeted before in July.
- In press reports there is **a lot of speculation** about whether or not foreign governments (e.g. Russia) were involved in these attacks (and in the previous recent attacks in Estonia and Lithuania) or if it is just the work of outraged citizens taking action on their own.
- **It is not clear however if these press reports have been confirmed by the Georgian government**. Some news reports suggest that the Georgian government have issued press releases confirming the above reports, but the source quoted (web-site of the Georgian Ministry of Foreign Affairs) does not substantiate these claims (no such press release listed). However, the presidential web-site had been moved to a hosting server in Georgia, U.S, which suggests that something – possibly an attack – has actually been taking place.
- It seems that the **assaults are not restricted to just government web-sites and not only limited to Georgian web-sites**. Moreover, some reports suggest that Georgia may be fighting back, attacking at least one Moscow-based newspaper site. Other commentators note that while there appear to be botnet attacks against .ge (the Georgian Top Level Domain) web-sites, the infrastructure providing Internet connectivity itself doesn't appear to have been directly attacked.
- Existing workarounds (including the use of emails and blogs for communication, as well as switching hosting locations and making copies of web-sites) were used. **The attacks came from a large number of sources all across the world**, suggesting a botnet (or multiple botnets) were behind them. As Georgia apparently does not have a governmental/ national Computer Security Incident Response Team (CSIRT), it is difficult to ascertain precisely which kind of counter-measures have been taken by the Georgian government.

2. ASSESSMENT AND ANALYSIS:

- In blogs and posts there are contradictory statements about the possible source of the Georgian DDoS. So far **there is neither enough nor reliable data** that indicates who actually might be behind the attacks. Unverified allegations range from active involvement of the Russian government itself in the Russian Business Network (RBN), a well known criminal network, to grass-root effects caused by 'hacktivists' or nationalistic vandals. One could even not finally exclude simply just overloaded services due to the increased popularity during some events in combination with not enough bandwidth.
- One aspect of the ongoing political and military conflict between Georgia and Russia that one would expect to see is the forging and falsifying of information and/ or averting and suppressing the propagation of 'official' information i.e. with the help of ICT and over the Internet. It is not possible yet to label the attacks as 'cyber warfare', as has been done by some.
- **Similarities with the Estonian event** have also been discussed on blogs and comparisons have been made. According to some security researchers "*compared to the May 2007 Estonian attacks these are more intense but have lasted (so far) for less time. This could be due to a number of factors, including more sizable botnets with more bandwidth, better bandwidth at the victims, changes in our observations, or other factors*". The **key difference,** of course, between what may or may not be happening at the moment in Georgia and what happened in Estonia and Lithuania is that **these attacks are happening in conjunction with a conventional conflict**. While the source of any attack has still to be confirmed, the possibility may exist that we are seeing cyber-attacks as an integral part of a coordinated military strategy rather than a 'stand-alone' source of political protest, inconvenience and/ or attempted economic loss for a country.

3. LINE TO TAKE:

- The Commission is aware of the various reports which suggest that certain web-sites in Georgia may have been subject to **large-scale cyber attacks from persons as yet unknown.**
- The issue is **primarily a matter of national sovereignty** and may well prove to be a matter of national security as well. **It would be inappropriate therefore for the Commission to comment further** in any detail in public at this point in time on what may or may not be behind the events in Georgia.
- **Because of the global nature of the Internet**, 'no man is an island' when it comes to Internet security and **each country**, inevitably, **has a degree of inter-dependence on other countries**, not least when it comes to responding these types of attacks. That said, there is a **heightened awareness** among policy makers of this type of event following the attacks on Estonia last year.
- These attacks are additional evidence therefore of the growing threat of cross-border cyber attacks and the need for a **reinforced incident response capability at EU-level**. Such capability would help to better coordinate and complement initiatives which are already implemented at national level. This is something that the Commission is already seeking to facilitate as part of the ongoing critical infrastructure protection initiatives at EU-level. To this end, the Commission intends to make proposals to the Member States at the beginning of 2009, taking full account of the important role and responsibility of the private sector and civil society organisations.

- Last but not least, it is useful to stress that Internet security and stability is a **shared** responsibility: governments, private sector and other involved actors need to each play their own role in optimising security and, where appropriate, to coordinate their activities to achieve this. Despite the impressive historical resilience and reliability of the Internet, it is **necessary to always continue to strengthen robustness wherever possible to combat the growing threats** increasingly faced by users and network operators world-wide. More cooperation, information and best practice sharing as well as partnership between public and private stakeholders, across sectors and geographical boundaries are needed.

DEFENSIVE POINTS:

Question: What is the Commission doing to protect critical information infrastructures such as the Internet?

- The Commission is working on a policy initiative (planned now for the beginning of 2009) on **Critical Information Infrastructure Protection (CIIP)** to engage Member States and private sector to enhance the level of **CIIP preparedness and response across the EU**. This work is carried out within the broader context of the European Programme on Critical Infrastructure Protection (EPCIP) whose main component is a proposal for a Directive on the identification and designation of European Critical Infrastructures. In June, the Council reached a political agreement on this Directive.
- The Commission has worked towards ensuring that **security and resilience of electronic communication networks** is a priority area for the activities of ENISA, the European Network and Information Security Agency. This approach was supported by Members States and has become a Multi Annual Thematic activity of ENISA.
- The Commission favours the establishment of governmental/ national Computer Security Incident Response Teams (CSIRTs), which are an important security resource and may constitute the key component of a **multi-lingual European Information Sharing and Alert Systems (EISAS)** whose idea was launched in 2006 by the Communication from the European Commission "A strategy for a secure Information Society".[8] The feasibility study of such an EISAS has been conducted by ENISA. Furthermore, JLS's 2008 programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 contained a call for proposals on prototyping EISAS. For the prototype of EISAS three competing projects are being funded.

Question: What is ENISA doing in order to support and facilitate Computer Emergency and Response Teams/ Computer Security Incident Response Teams (CERTs/ CSIRTs)?

- ENISA had not been mandated an operational task by the regulation that established the Agency. However, ENISA has an important role to play in enhancing network and information security.
- ENISA has established an **ad-hoc Working Group on Computer Emergency Response Teams (CERTs)**. Since the very beginning ENISA's experts were in close contact with all relevant communities in Europe and beyond. ENISA published material on setting-up and cooperation of CSIRTs as well as best practices for running CSIRTs. ENISA is also organising yearly CERT workshops on specific topics.
- The level of security and resilience of the communication and information infrastructures in any Member State heavily depends on the security and protection provided outside its national borders. Many of the challenges and the issues faced by

[8] "A Strategy for a secure Information Society – dialogue, partnership and empowerment" COM(2006) 251.

Member States will be common and thus a coordinated approach will benefit all. In this context, one of **ENISA's activities** foreseen in the draft work programme 2009 **concerns incident response capabilities at National level and a pan European cooperation of those capabilities are vital to for the EU**. The intention is to invite Member States to establish/ reinforce national incident response capability as a key resource for preparedness.

- **ENISA could significantly support the process towards an EISAS by engaging Member States in close cooperation**.

4. PUBLICLY AVAILABLE DATA SOURCES:

On-line press:
http://www.tagesschau.de/ausland/georgien366.html
http://www.theregister.co.uk/2008/08/11/georgia_ddos_attack_reloaded
http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/
http://news.cnet.com/8301-1009_3-10015657-83.html?tag=nl.e703
http://news.cnet.com/8301-1009_3-10016152-83.html
Georgian Ministry of Foreign Affairs (press releases):
http://www.mfa.gov.ge/index.php?sec_id=461&lang_id=ENG&limit=40
Blogs & posts:
http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.htmlb
http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080720
http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080811
http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080812
http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813)
http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/
http://arstechnica.com/news.ars/post/20080813-georgian-attacks-might-not-be-russians-after-all.html
http://www.circleid.com/posts/88116_internet_attacks_georgia/
http://www.circleid.com/posts/88137_georgians_use_spam/
http://www.circleid.com/posts/88123_updates_georgian_cyber_attacks/
http://www.circleid.com/posts/88124_russian_cyber_attacks_precede_military_action/
http://stupid.domain.name/node/685
http://stupid.domain.name/node/687
http://www.sophos.com/blogs/gc/g/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/

ANNEX 18 C: DETAILS OF A MAJOR SECURITY VULNERABILITY AFFECTING THE INTERNET DOMAIN NAMING SYSTEM PUBLICLY DISCLOSED

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 4 September 2008

FLASH REPORT

DETAILS OF A MAJOR SECURITY VULNERABILITY AFFECTING THE INTERNET DOMAIN NAMING SYSTEM PUBLICALLY DISCLOSED

1. WHAT HAPPENED?

- According to press reports dated from July 9th and to an official "security advisory" by the US Computer Emergency Readiness Team (US-CERT) of July 8th, a major vulnerability in software products which provide a basic infrastructural service on the Internet was discovered by Dan Kaminsky, a known security researcher.

- The problem affects several implementations of so-called "DNS servers". DNS servers provide users on the Internet with "naming" functionalities: upon request of a user, or of a user's computer/browser, they translate a name, such as http://ec.europa.eu/, into a numerical address that identifies a device connected to the Internet, such as 151.34.25.2.

- According to the official security advisory by US-CERT, to ongoing discussions that have been taking place on security researchers' fora and to the official presentation by Dan Kaminsky at the Black Hat 2008 conference (Las Vegas, 2008, 2-7 August 2008) the vulnerability allows an external attacker, under certain conditions, to alter the information that affected "DNS servers" return when performing the name-address translation. This could entail, for example, that when the user visits http://ec.europa.eu/, a website controlled by someone else than the European Commission would appear. The different website, using similar graphics and text, could pretend to be this website and thus mislead the user.

2. ASSESSMENT AND ANALYSIS:

- This kind of security problem – technically known as "cache poisoning" – has been known for a number of years as being both theoretically and practically possible. The same US-CERT has issued an advisory on the very same problem in 1997.

- As already mentioned the vulnerability could have the effect that users of the affected "DNS servers" could possibly be directed to fake web sites without realizing it. Similar effects can take place in whatever system on the Internet relies on the global DNS system for name-address resolution. Due to the pervasive and fundamental role of such system for the Internet as a whole, e-mail exchanges, instant messaging, possibly "Voice over IP" systems, and other services can be affected, unless the concerned web site or other online service uses strong authentication technologies – usually based on cryptography – to certify they are who they really claim. Most e-commerce web-sites use this kind of authentication mechanisms. E-mail and "Voice

over IP" systems, for the time being, do not seem to widely use strong authentication systems.

- The text of the July 8th US-CERT advisory suggested that the vulnerability might be a "refinement" of this old problem, possibly using a combination of known techniques to make potential attacks quicker and less costly for the attacker.

- On August 6th, as announced, Dan Kaminsky extensively discussed the details of his findings at the Black Hat 2008 conference – one of the top-rated security conferences across the globe – in Las Vegas, USA. A link to the slides is provided in section 4 of this report, together with a link to a thorough – and more easily understandable – analysis of Kaminsky's discovery.

- The vulnerability indeed relies on known flaws in the implementation of many DNS servers. Such weaknesses – lack of strong randomisation in the generation of the "query IDs" and in the choice of "source UDP ports" (see the links to the slides presented by Dan Kaminsky and to their analysis in section 4 for more details) – could be combined in order to "hijack" entire domain names. According to some tests, a vulnerable DNS server could be exploited in less than 10 seconds.

- According to the analysis of Dan Kaminsky, it is not sufficient to rely on strong authentication based on encryption – common on the World Wide Web in the form of the SSL (Secure Sockets Layer) protocol – together with an infrastructure through which "Certification Authorities" (CA) distribute the "certificates" which ensure a party is really communicating with the other intended party. This is due to the fact that, according to Kaminsky's research, the process for obtaining a certificate from a CA is often not secure enough and, in some cases, only necessitates email communication between the requestor and the CA: as mentioned above, the DNS vulnerability discussed here can be used to intercept email traffic as well.

- Precise data on the number of affected DNS systems and on the rate of fixing of vulnerable systems is not currently available. CERT.at, the Austrian national Computer and Emergency Response Team, has conducted an analysis on a number of Austrian DNS servers: on August 15, around 50% of Austrian DNS servers were still vulnerable. NASK, which hosts CERT Polska, has estimated that as of 31 July 2008, 69% of Polish DNS servers were still vulnerable.

- There seems to be a general consensus amongst the concerned stakeholders that DNS-SEC – the secure version of the DNS system, based on strong cryptography for authentication – is the only long-term solution to this vulnerability and to other similar ones that might appear in the future.

- Although this vulnerability, contrarily to early reports, is indeed significantly different from others that have been known for a long time, it looks like the mitigation strategies that have been suggested – which include increasing the randomisation of "query IDs" and the implementation of "source UDP port randomization" (see the links to the slides presented by Dan Kaminsky and to their analysis in section 4 for more details) – should have already been implemented as a "best practice" by vendors since some years.

- The fact that a significant segment of the industry is still selling and using software which does not implement such "best practices" begs the question whether the industry had the necessary incentives to do so – and, if not, which incentives would have been needed (and will be needed in the future) to ensure such result.

- It is worth to reflect on the large number of "affected vendors", i.e. vendors whose "DNS servers" are vulnerable, that the latest US-CERT security advisory refers to: more than 70. Although the vulnerability is due to a design, rather than implementation, flaw, it is nonetheless possible to hypothesise that a reason for such a large number of vendors to be affected by a single vulnerability is that most of them are using the same "code base", i.e. the same software product or library, in order to provide their services. It is a useful reminder of the importance of heterogeneity and diversity of systems – coupled with their interoperability – as a strong component of a secure information society.

3. LINE TO TAKE:

- The Commission has been aware of the vulnerability as soon as the CERT advisory was published and has been closely following the discussions in the security community.

- The fact that precise information on the exact nature of the vulnerability was made publicly available only after several weeks of the official CERT advisory raises several questions of interest to all the stakeholders in the EU. Although confidentiality and security concerns are absolutely understandable, it is worth reflecting on the need for all the interested stakeholders to be promptly and fully informed of relevant technical details of any security threat, using the proper procedures and tools to ensure a trusted and secure exchange of data.

- More specifically, there is a need to reflect and discuss as widely as possible on who are the "interested stakeholders" in this kind of situations. Assuming that detailed information should be made available only to a restricted "trusted circle" of players, the question becomes who should be a part of this "trusted circle" – which public bodies, which countries, which private companies? Moreover, it is worth reflecting on the best way to ensure that the ones outside the "trusted circle" are not put at a commercial or political disadvantage.

- It is also striking to note the extremely large numbers of software vendors affected by this vulnerability. This prompts the question whether we are in front a "software monoculture" problem, where only one or two different software implementations are used throughout the industry, thus worsening the security impact when such implementations are found to be vulnerable, as in this case.

DEFENSIVE POINTS:

Question: what is the Commission doing to ensure the security and stability of the Internet?

- The Commission is actively engaged in developing a European programme for the protection of critical communications and information infrastructure, including the Internet. This work is carried out within the broader context of the European programme on Critical infrastructure protection.

- In the context of DG Justice, Liberty and Security 2008 programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, a project aimed at strengthening the resilience of the

European DNS infrastructure is currently being negotiated. The project aims to achieve such target by coordinating analysis efforts across the European Union and providing tools and policies for a proper sharing of information amongst all concerned stakeholders.

- The Commission has worked towards ensuring that **security and resilience of electronic communication networks** is a priority area for the activities of ENISA, the European Network and Information Security Agency. This approach was supported by Members States and has become a Multi Annual Thematic activity of ENISA.

- Discussions related to Internet security took place in a workshops, at the initiative of the European Commission, on lessons learnt from large scale attacks on the Internet on 17.01.08. The participants underlined that Internet security and stability is a **shared responsibility.** They stressed the fundamental necessity to build further the resilience and robustness of the Internet; **response preparedness is equally crucial**. **More cooperation, information and best practice sharing** as well as partnership between public and private stakeholders, across sectors and geographical boundaries are needed.

- One key element of an overall strategy to ensure the security and stability of the Internet is to avoid the "monoculture" problem, where one or very few software implementations are used throughout the industry. The Commission has already stressed, in its Communication (COM(2006) 251 – "A strategy for a Secure Information Society – "Dialogue, partnership and empowerment") how the emergence of certain "monocultures" in software platforms and applications can greatly facilitate the growth and spread of security threats, and how diversity, openness and interoperability are integral components of security and should be promoted.

4. PUBLICLY AVAILABLE SOURCES:

Press reports:
http://technology.timesonline.co.uk/tol/news/tech_and_web/article4301557.ece
http://www.guardian.co.uk/technology/2008/jul/10/hacking.internet
http://afp.google.com/article/ALeqM5hwFqcnWAuDWlcqfvfyHu5PGG9RMQ
http://news.bbc.co.uk/2/hi/technology/7496735.stm
http://www.pcworld.com/businesscenter/article/148151/internet_bug_fix_spawns_backlash_from_hackers.html
http://www.latribune.fr/info/Une-menace-mondiale-pour-la-securite-d-Internet-a-ete-evitee-~-ID614514B8D2C764C0C125748100580728-$Channel=Entreprises%20%26%20secteurs-$SubChannel=Communication
http://www.lemondeinformatique.fr/actualites/lire-les-grands-des-tic-s-allient-face-a-une-faille-des-dns-26548.html

The official US-CERT advisory:

http://www.kb.cert.org/vuls/id/800113

The old CERT advisory, highlighting the (allegedly) same type of vulnerability:

http://www.cert.org/advisories/CA-1997-22.html

Slides of Dan Kaminsky's presentation at Black Hat 2008:

http://www.doxpara.com/DMK_BO2K8.ppt

"An Illustrated Guide to the Kaminsky DNS Vulnerability" – analysis of Kaminsky's discovery:

http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

CERT.at analysis:

http://cert.at/static/cert.at-0802-DNS-patchanalysis.pdf
http://cert.at./static/cert.at-0802-bis-DNS-patchanalysis-update.pdf
http://cert.at/static/cert.at-0802-DNS-patchanalysis-aug18.pdf

CERT Polska analysis:

http://www.dns.pl/english/cachepoisoning_en.html

ANNEX 18 D: NEW ATTACK REVEALING FUNDAMENTAL FLAW IN THE TCP PROTOCOL

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 28 October 2008

FLASH REPORT

New attack revealing fundamental flaw in the TCP protocol

1. WHAT HAPPENED?

- According to press reports dated from October 1st 2008, two Swedish researchers, from Swedish security firm Outpost24, claim to have discovered a new attack possibility that could disrupt any computer that uses the TCP protocol (Transmission Control Protocol). The TCP protocol associated with the Internet Protocol (IP) is used by computers to communicate with each other. And it is fundamental to the functioning of the Internet.

- The two researchers claim that they have developed a software tool to demonstrate the attack. The tool can be exploited to cause denials of service and resource consumption on virtually any machine that is in a "listening" mode, waiting for the initiation, by another computer, of a TCP-based communications. All the web servers on the Internet are actually in this situation ready to receive TCP-based communications at the request of the computers of users who browse websites hosted by the web server.

- The two researchers claim that they have not seen a single implementation of the TCP protocol that was not vulnerable, meaning that the problem affects all operating systems.

- The researchers mentioned that after keeping the flaw quiet for years, they hope that going public will raise awareness and help accelerate the creation of a solution. Another reason reported is that the researchers are concerned that the migration toward IPv6 could aggravate the situation because IPv6 services appear to be more affected by the fact that they require more resources (in particular to handle larger IP addresses).

- The Finnish Computer Emergency Response Team (CERT-FI) is coordinating research into the security issue and providing information to software vendors affected.

- Based on the few indications provided by the Swedish researchers, several security experts, as reported in specialised blogs and as contacted by EC, have emitted doubts on the actual severity of this new threat. The exploited vulnerability seems to be well-known. This analysis was publicly confirmed by CISCO. While experts agree that it is entirely possible that the researchers have found improved/optimized versions of a well-known attack, **they do not consider it as a serious threat to the Internet as a whole**. **They do however consider it an important issue which should be fixed**.

2. ASSESSMENT AND ANALYSIS

- The few elements provided by the two researchers indicate that this "new" attack possibility would take the form of a Denial of Service and resource consumption attack. Security experts speculated that this seems to boil down to the well known issue of the non-infinite capability of servers to handle several running connections at the same time.

- Regarding Denial of Service attacks, effective ones are already commonplace. This has been demonstrated by the cyber attack targeting Estonian Internet resources last year. The attacks used to affect the Estonian Internet resources were based on a simple method of "brute force" that floods the target with a large volume of requests, distributed among a large span of sources. According to security experts, "brute force" Denial of Service attacks are certainly much more effective and difficult to deter than what seems to be a more sophisticated attack targeting the TCP protocol.

- This is based on the assumption that for the current attack, the attacker's computer initiate a multitude of communications with the target computer that are never completed by the attacker, using resources within the target computer. If the maximum number of connections is established in this way, the server is no longer able to respond to other clients' connection requests because earlier connections have not been terminated.

- During this attack the IP address of the source has to remain the same so that the communication can be established. Therefore, once the attack has been identified, the mitigation proposed by CERT-FI is to block the IP address of the attacker. According to the Swedish researchers however, it might be difficult to detect the attack that, from the target side, might looks like intense but normal activities.

- The specificity of this attack is that, according to the two researchers, it can be performed from a very low bandwidth connection. There is no need for the attacker to have access to large capacity connections. This statement also tends to confirm however, that such a type of attack, once detected, can be easily stopped by blocking the source IP address.

- **All these elements concur to conclude that this new attack seems not adding much to the already serious threat landscape on the Internet**. While the distributed and open nature of the Internet is recognised as contributing to its flexibility and resilience, this event highlights once again the structural vulnerability of the Internet that is based on protocols which were not specifically designed for extremely hostile environments where not all the actors are fair players. **The structural vulnerabilities of the Internet should therefore continue to receive the appropriate level of attention by the global Internet community**.

- Furthermore, it is interesting to note that this flaw has been announced publicly with the promise of further disclosure at a forthcoming security conference event. The possibility that the announcement has an element of "marketing" in it cannot therefore be discounted.

3. LINE TO TAKE:

- The Commission is actively engaged in developing a European programme for the protection of Critical communication and Information Infrastructures Protection (CIIP), including the Internet, planned for the beginning of 2009. Several areas of

action which are currently under consideration will be relevant for the management of such vulnerabilities.

- One area for action currently being considered is the improvement of the incident response capability at national and European level. The intention is to invite Member States to establish and reinforce national incident response capability, possibly built on National/Governmental CERTs/CSIRTs, as a key resource for preparedness, information sharing, coordination and incident response. This flaw has demonstrated the key role of a CERT in handling the coordination between researchers and software vendors to find a solution as well as to manage the disclosure process.

- Another area for action currently being considered is the development of a trusted public-private partnership (PPP) at the European level on security and resilience to support information sharing and dissemination of good practices. It is to be considered whether such partnership could help in improving the exchange of reliable information between security experts and policy makers on Internet vulnerabilities. The PPP could also discuss 1) how to engage the concerned stakeholders (researchers, CERTs etc…) in respecting fair-play principles while sorting out a solution and disclosing potentially valuable information to third parties and 2) anticipate the operational needs and set the conditions for fulfilling these needs in particular concerning tools to exchange the details of vulnerabilities and threats in an environment of confidentiality and trust.

- Eventually, the initiative will propose to enhance the global cooperation to discuss EU priorities for Internet long term stability and resilience in particular for what concerns Internet critical components (including its communication protocols), the overall architecture, the governance and, last but not least, international arrangements for remedial, mutual assistance and recovery.

- The Commission should continue to raise awareness on the risk of the emergence of certain “monocultures” in ICTs platforms and promote diversity, openness and interoperability as integral components of security and resilience as proposed in the 2006 strategy for a Secure Information Society (COM(2006) 251).

- Furthermore, the Commission has worked towards ensuring that **security and resilience of electronic communication networks** is a priority area for ENISA, the European Network and Information Security Agency. This approach was supported by Members States and has become a Multi Annual Thematic activity of ENISA.

4. PUBLICLY AVAILABLE SOURCES:

CERT-FI statement: https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html

CISCO statement: http://www.cisco.com/warp/public/707/cisco-sr-20081017-tcp.shtml

Transcript of an interview of the two researchers: http://www.curbrisk.com/security-blog/outpost24-tcp-denial-of-service-vulnerability-interview-transcript.html

Explanations from an other expert: http://insecure.org/stf/tcp-dos-attack-explained.html

Press reports:

http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1332898,00.html

http://blog.robertlee.name/2008/10/clearing-up-some-factual-inaccuracies.html

http://www.arnnet.com.au/index.php/id;650063178;fp;4;fpid;1382389953

http://www.pcsympathy.com/2008/10/01/researchers-uncover-major-ip-flaw/

http://www.darkreading.com/blog.asp?blog_sectionid=403&doc_id=164939&WT.svl=tease2_2

ANNEX 19: WORKING DOCUMENT ON THE ECONOMIC IMPACTS OF CYBER-ATTACKS AND CYBER-DISRUPTIONS

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

WORKING DOCUMENT

June 2008

Economic Impacts of Cyber-Attacks and Cyber-Disruptions

DISCLAIMER
This report does not necessarily represent the views of the Commission

TABLE OF CONTENTS

INTRODUCTION

The current report is an internal working document prepared by DG INFSO. Its purpose is to compile data on economic impacts of cyber attacks and disruptions drawing from a wide variety of public available sources. This compilation refers to data reviewed before June 2008.

Notes and references to the sources which are directly cited appear as footnotes in the main text. In addition, a bibliography of further materials consulted is available at the end of the document.

1. DEPENDENCE OF SOCIETY ON INFORMATION AND COMMUNICATION INFRASTRUCTURES

In order to assess the macroeconomic effects of a disruption of critical communication and information infrastructures it may first be useful to examine how these infrastructures contribute to economic activity since it is that contribution that is presumed to be at most risk.

The Internet is a worldwide network of networks. Everywhere in the world, people more and more rely on the Internet for the performance of various activities.

Internet-based applications underlie major advances in science, business organisation, environmental monitoring, transport management, education and e-government. There is every reason to think that in the future, the network of networks will continue to reach further into our daily lives and into other infrastructures which we rely on. Whereas the Internet now connects just over a billion people, in the future it will potentially connect many billions of objects, from refrigerators to recycling bins[1]. Thus, one can naturally ask oneself – what would be the impact on society if the functioning of the Internet would be severely disrupted. Which parts of society would be affected and to what extent? To what degree are we dependent on the well functioning of ICT networks (most notably but not only the Internet) in performing our daily activities?

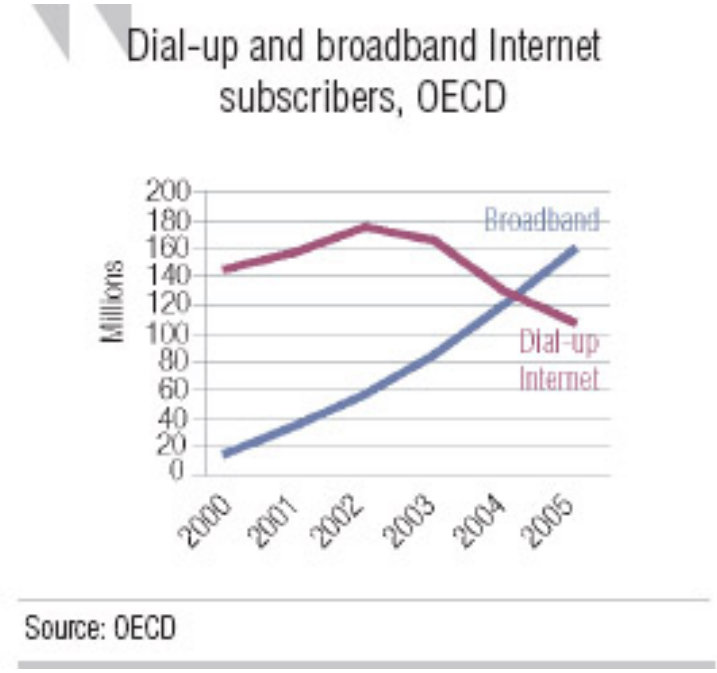
The pervasiveness of the Internet in business functions means that a cyber catastrophe will mean that: The effects will be serious and far-reaching, affecting – directly or indirectly – nearly every public institution, business and citizen.

The current survey attempts to assess the dependence of our society on the information and communication networks, and to quantify the potential impact a major disruption would have on the different stakeholders and the society as a whole.

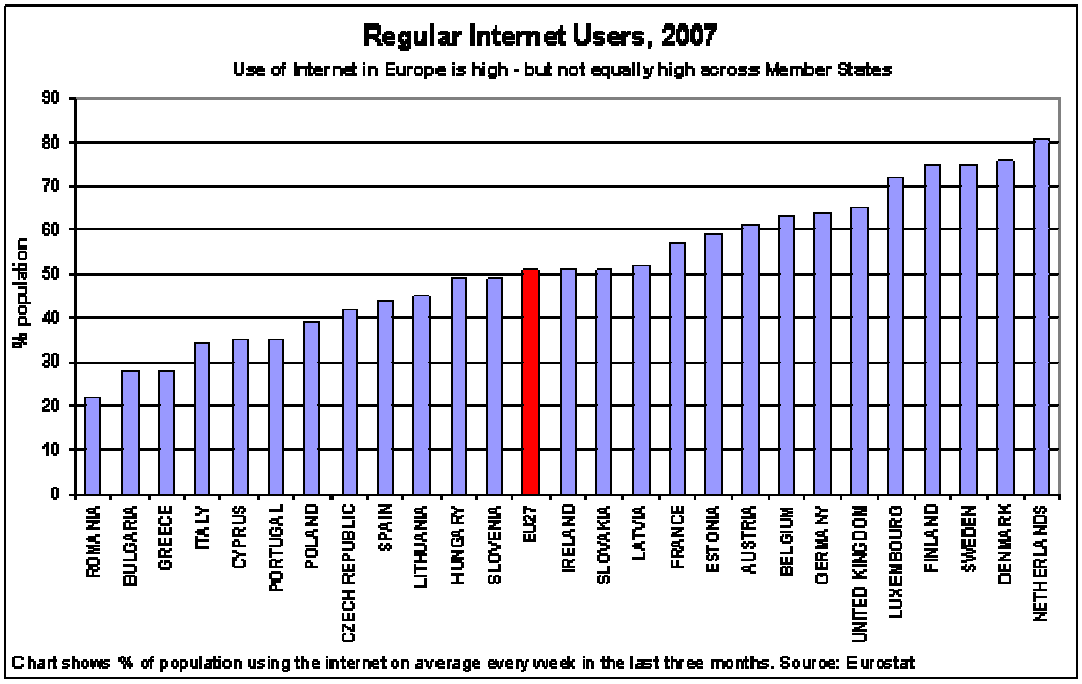
[1] Huttner, S., The Internet economy: Towards a better future, OECD Science, Technology and Industry Directorate, http://www.oecdobserver.org/news/fullstory.php/aid/2330/The_Internet_economy:_Towards_a_better_future_.html

a. Internet usage by citizens

Millions of people now use the Internet for everything from doing homework to buying books, or playing or downloading games, music and movies. Users are accessing the Internet via all manner of wireless devices, from laptops to mobile phones. Along the way, communications became the fastest-growing part of household expenditure since 1993, even faster than health and education. Levels of user participation and publication on the Internet have also surged, from blogs, podcasts and interactive wikis that anyone can modify, through to services for sharing photos and video clips, such as Flickr and Daily Motion. Social networking sites such as Bebo, Facebook and MySpace represent another rapidly developing frontier of communication.



According to Eurostat figures for 2007, more than 50% of the EU population are regular users of the Internet.



Source: Community Survey of ICT Usage in Households and by Individuals, 2007 Eurostat

Moreover, the share of regular users has grown up steadily in the recent years, marking a 40% increase in comparison to 2004:

Share of individuals regularly using the Internet - Percentage of individuals who accessed the Internet, on average, at least once a week				
	2004	**2005**	**2006**	**2007**
EU (27 countries)	36	43	45	51
EU (25 countries)	38	43	47	53

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

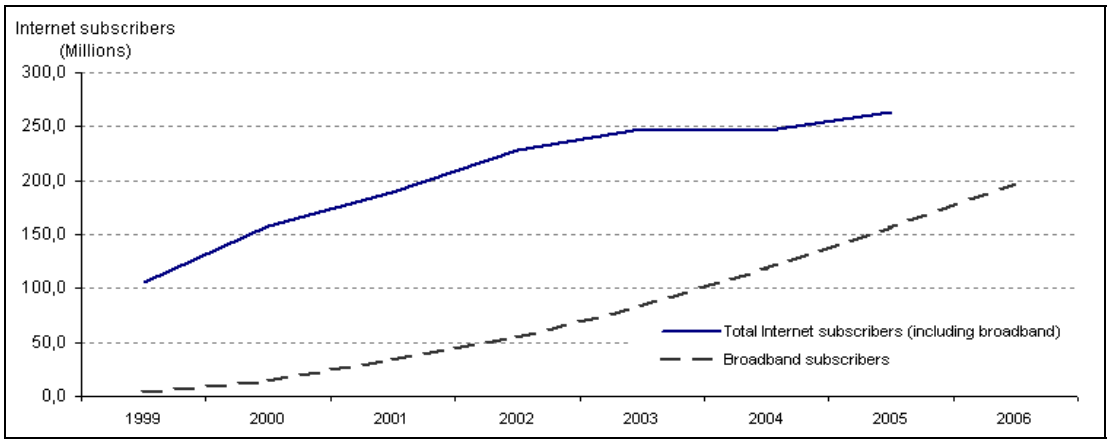
In addition, the majority of EU households now have Internet access at home, and, if the trend from the last years is preserved we can expect a very high penetration rate in the near future.

Level of Internet access - households - Percentage of households who have Internet access at home						
	2002	**2003**	**2004**	**2005**	**2006**	**2007**
EU (27 countries)	:	:	40	48	49	54
EU (25 countries)	:	:	42	48	51	56
EU (15 countries)	39	43	45	53	54	59
Euro area	36	40	43	50	51	56

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

Similar trends are revealed for the OECD countries, which have achieved more than twofold increase in the number if Internet subscribers between 1999 and 2006[2]:

Internet subscribers in total for OECD, millions



Another data source[3] shows that the majority of the EU Member States (MSs) rank high on world level in terms of Internet usage per capita.

Internet usage per 100 inhabitants

Rank	Country	Score
1	Netherlands	88.87
3	Sweden	76.97
5	Luxembourg	72.01
12	Slovenia	63.62
13	Switzerland	60.02
15	Norway	58.48
16	Denmark	58.23
17	Estonia	57.36
18	United Kingdom	56.03
19	Finland	53.34
21	Austria	51.19
22	Italy	49.63
23	France	49.57
24	Germany	46.67
25	Latvia	46.65
27	Belgium	45.67
29	Spain	42.83
30	Cyprus	42.23
31	Slovak Republic	41.76
34	Hungary	34.75
35	Czech Republic	34.69

[2] OECD Key ICT indicators, www.oecd.org/sti/ICTindicators

[3] Global Information Technology Report 2007-2008 (Data Source: International Telecommunication Union, World Telecommunication Indicators 2007) ,http://www.insead.edu/v1/gitr/wef/main/analysis/framework.cfm

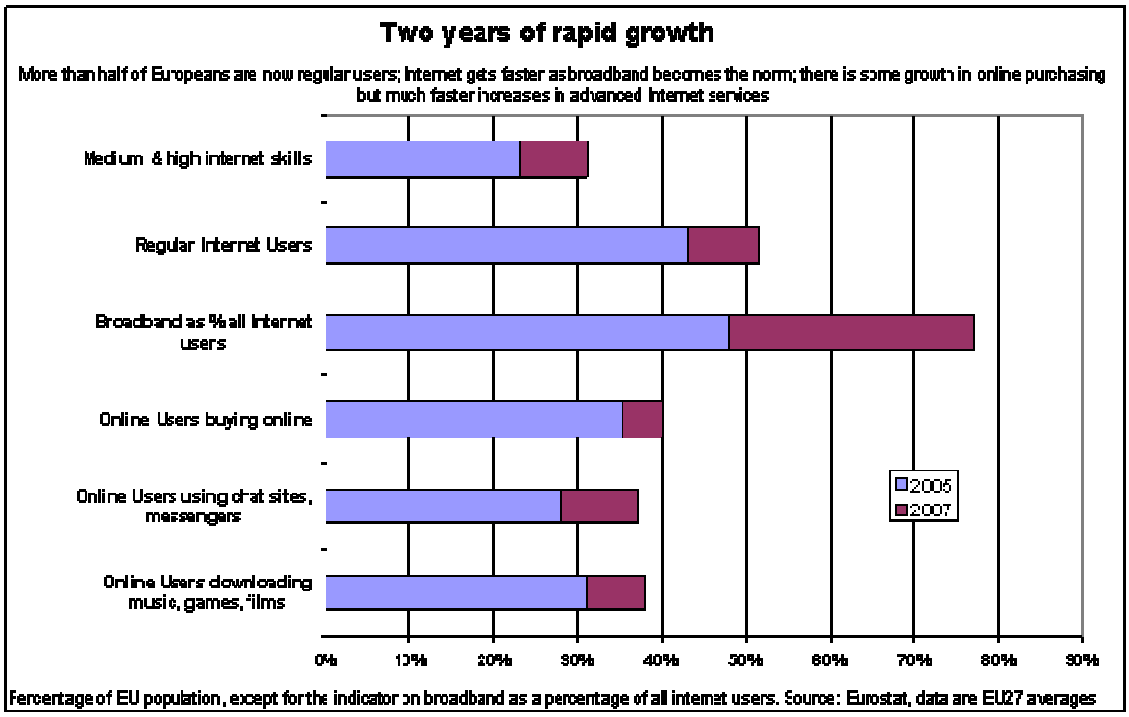
38	Ireland	34.13
39	Romania	32.36
40	Malta	31.73
41	Lithuania	31.69
42	Portugal	30.47
44	Poland	28.57
49	Bulgaria	24.38
60	Greece	18

The same source shows also that the number of personal computers per capita is quite high.

Share of personal computers per 100 inhabitants

Rank	Country	Score
4	Netherlands	85.55
5	Sweden	83.49
7	United Kingdom	76.52
9	Denmark	69.46
12	Luxembourg	62.37
13	Austria	61.12
14	Germany	60.47
15	Norway	59.41
17	France	57.86
20	Ireland	52.99
22	Finland	50.01
23	Estonia	48.91
25	Slovenia	41.08
26	Belgium	37.62
27	Italy	36.99
28	Slovak Republic	35.72
29	Cyprus	33.41
30	Spain	28.11
31	Czech Republic	27.40
32	Latvia	24.53
33	Poland	23.99
41	Lithuania	17.98
44	Malta	16.61
46	Hungary	14.90
50	Portugal	13.40
52	Romania	12.96
61	Greece	9.17
70	Bulgaria	6.34

Furthermore, European citizens are quickly improving their digital skills – over the past two years 8% of the EU population improved their Internet skills to medium and high[4]. This is a strong premise for further increase in usage in the future.



Source: Community Survey of ICT Usage in Households and by Individuals, 2007. Eurostat

The Internet access in schools[5], which is important for developing the ICT skills of the young generation, has been on the rise as well. The following table shows that the majority of the EU countries rank high in ensuring Internet access to students.

Internet access in schools
(1 = very limited; 7 = extensive most children have frequent access)

Rank	Country	Score
2	Finland	6.35
3	Sweden	6.34
5	Denmark	6.21
6	Estonia	6.19
8	Austria	6.09
11	Netherlands	5.98
14	United Kingdom	5.78
18	Malta	5.51
19	Luxembourg	5.51
20	Slovenia	5.47
23	Czech Republic	5.26

[4] http://ec.europa.eu/information_society/eeurope/i2010/infso_today/index_en.htm

[5] Global Information Technology Report 2007-2008, Data Source: World Economic Forum Executive Opinion Survey 2006 2007, http://www.insead.edu/v1/gitr/wef/main/analysis/framework.cfm

24	Germany	5.22
25	Belgium	5.20
27	Hungary	5.09
28	France	5.05
29	Portugal	5.02
32	Lithuania	4.88
34	Latvia	4.82
36	Slovak Republic	4.69
38	Ireland	4.57
41	Spain	4.39
42	Croatia	4.25
48	Poland	3.87
49	Romania	3.82
53	Bulgaria	3.71
54	Italy	3.69
61	Greece	3.47

b. Internet usage by businesses

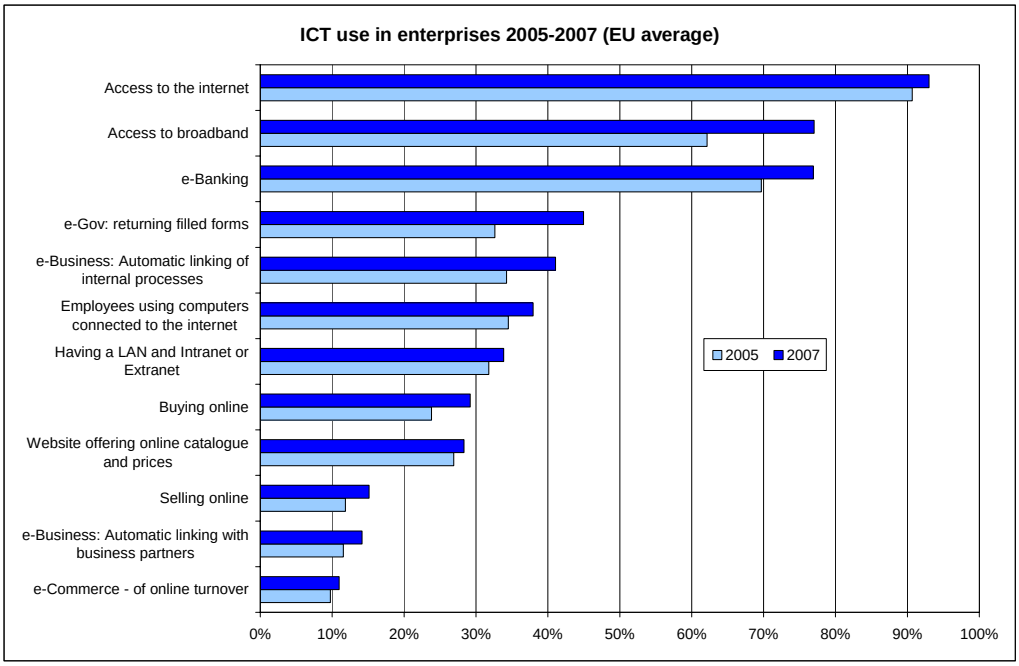
Internet usage by EU businesses of all sizes has grown rapidly in the past decade, and Internet dependence has penetrated every corner of the economy. Different studies show that the larger the business, the greater the reliance

Connectivity and basic ICT uptake have strongly progressed in recent years. By 2007 93% of the EU businesses had access to the Internet compared to 88% in 2004.

Share of enterprises having access to the Internet					
geo	**2003**	**2004**	**2005**	**2006**	**2007**
EU (27 countries)	:	88	91	92	93
EU (25 countries)	:	89	91	93	95
EU (15 countries)	85	91	92	94	95
Euro area	87	90	92	94	95

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

Enterprises make use of ICT extensively in their activities for a variety of purposes. 77% were using the Internet for dealing with banks. In addition, enterprises started making significant use of e-government services, stimulated by progress in the greater availability and sophistication of online public services:



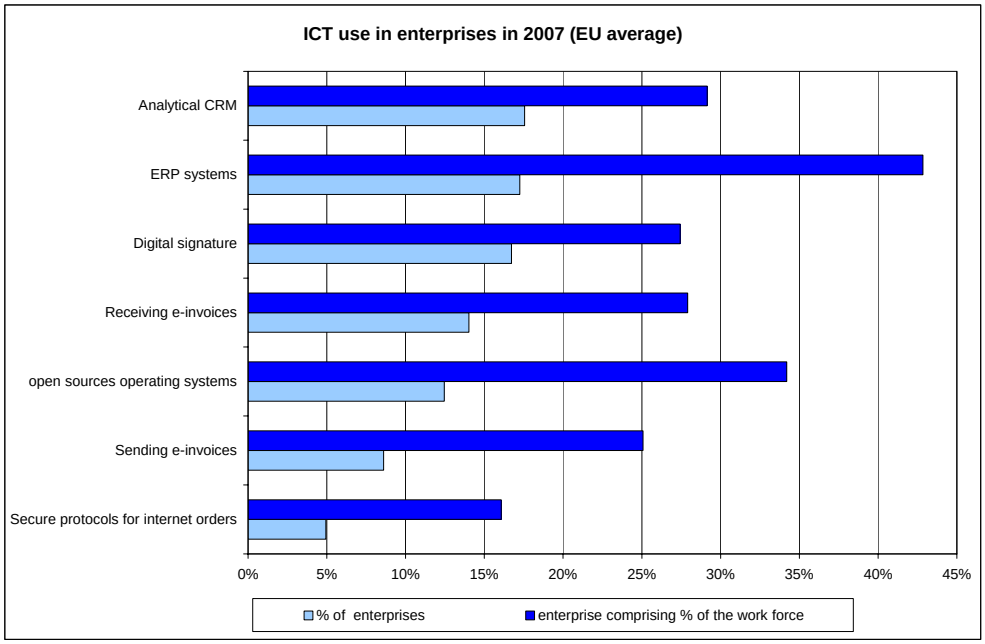
Source: Eurostat, Survey on ICT use in EU enterprises. Data refer to all the enterprises, excluding the financial sector. [6]

The deployment of ICTs in business processes requires significant investment, which is more likely to be carried out by large organisations. Investment requirements are one of the main sources of the gap in ICT take-up between SMEs and large businesses.[7] Therefore, data weighted by enterprise size indicate that the impact of ICTs on the economy is even larger than suggested by aggregate un-weighted data[8].

6 All the indicators listed in the chart are expressed in terms of % of enterprises, except for online turnover (as % of total enterprise turnover) and the % of employees using computers connected to the Internet (as % of total employment)

7 SEC(2008)470, http://ec.europa.eu/information_society/eeurope/i2010/docs/annual_report/2008/sec_2008_470_Vol_1.pdf

8 The weighting factor is the number of persons employed. Statistics weighted by enterprise size have been made available by Eurostat starting from the 2007 edition of the survey.



Source: Eurostat, Survey on ICT use in EU enterprises [9]

For example, the use of digital signature is limited to 17% of all enterprises, but these same businesses employ more than one quarter of the workforce in the EU. Overall, the uptake of e-invoicing is still low in the EU: only 9% of enterprises (representing the 25% of the economy) are sending them to their business partners. Obstacles include lack of standardisation, legal uncertainty, especially in international transactions, and lack of affordable software solutions. However, the take-up of e-invoicing is a good example of the gaps and differences across Member States. While in Northern countries enterprises sending e-invoices represent more than 40% of their economies, in most of the new Member States the move from paper to electronic invoices has just started.

On global level, the EU countries take forefront positions with respect to Internet use in their business activities:

Companies in your country use the Internet extensively for buying and selling goods and for interacting with customers and suppliers (1 = strongly disagree 7 = strongly agree)

Rank	Country	Score
2	Estonia	6.10
3	Sweden	5.96
4	United Kingdom	5.95
5	Germany	5.90
7	Denmark	5.81
8	Switzerland	5.69
12	Netherlands	5.62
13	Finland	5.60

[9] Employment weighted figures on the use analytical CRM (Customer Relationship Management) have been estimated by Commission services on the basis of Eurostat data.

15	Norway	5.52
16	Austria	5.48
20	Czech Republic	5.27
23	France	5.09
24	Ireland	5.03
26	Belgium	4.94
30	Luxembourg	4.76
32	Malta	4.71
33	Lithuania	4.67
34	Slovenia	4.58
36	Portugal	4.50
38	Poland	4.42
39	Latvia	4.34
46	Spain	4.20
48	Cyprus	4.18
49	Slovak Republic	4.18
50	Hungary	4.17
54	Italy	4.10
78	Romania	3.65
87	Bulgaria	3.49
97	Greece	3.30

Source:Global Information Technology Report 2007-2008 (data based on: World Economic Forum Executive Opinion Survey 2006 2007)

Another survey[10], done for the UK, confirms that IT systems and in particular Internet, are increasingly important to business operations. Nearly every UK business makes use of the Internet; 97% have an Internet connection and 88% of these are broadband. 81% of companies have a web-site, with 89% of these being externally hosted. In addition, dependence on IT continues to grow with as only one in twenty large companies (and no very large ones) and one in six small companies could operate their businesses without their IT systems.

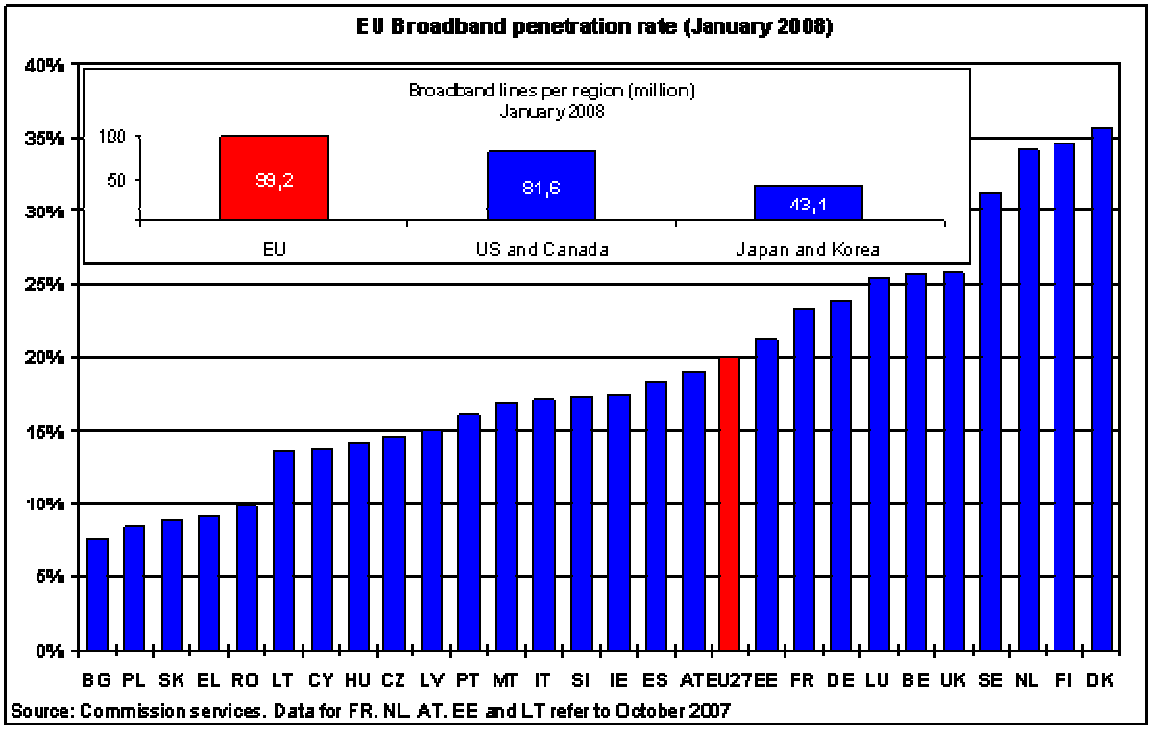
c. Broadband penetration

High-speed broadband connection is becoming the norm in the EU. The broadband sector generated estimated revenues of €62 billion; 19 million broadband lines were added in 2007, which is the equivalent of more than 50,000 households every day.[11] Overall, nearly 80% of all Internet connections are broadband, as compared to less than 50% in 2005. By January 2008, 20% of Europeans had broadband connections, which is

[10] Information security breaches survey 2006, DTI

[11] COM(2008) 153 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions – Progress Report on the Single European Electronic Communications Market 2007

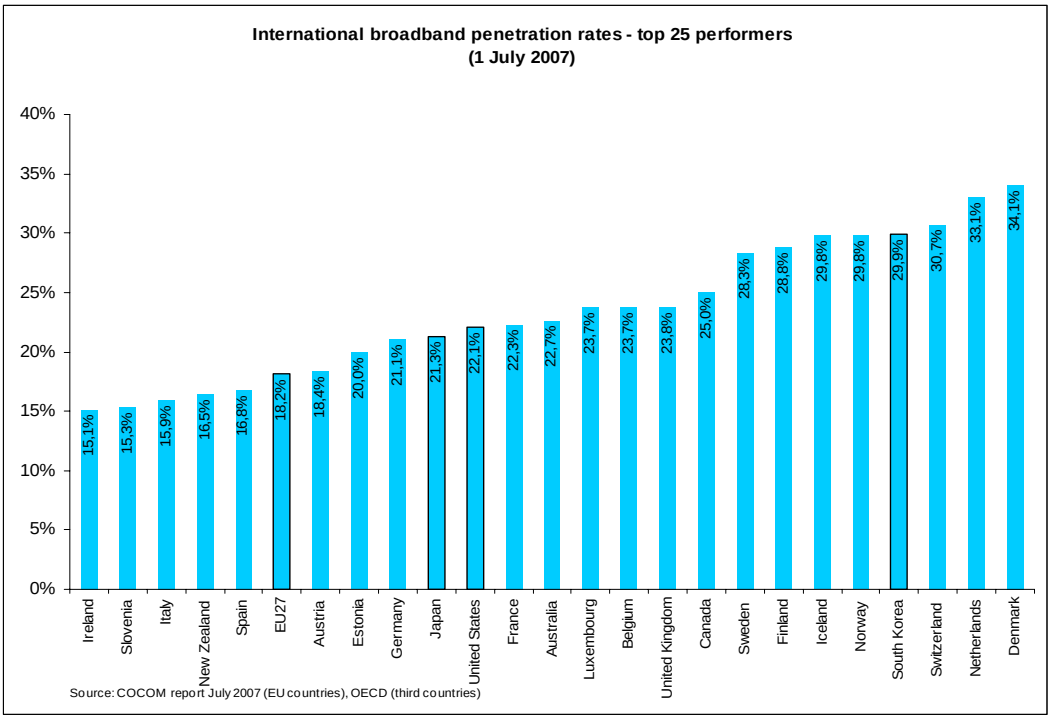
a threefold increase since the Union's enlargement in 2004. Progress is being registered in all the Member States.



Source: Commission services, based on data from COCOM and Point Topic.

Denmark, Finland, the Netherlands and Sweden are world leaders in broadband deployment with penetration rates over 30% at the end of 2007, according to the European Commission's 13th Progress Report on the Single Telecoms Market[12]. These EU countries, together with the United Kingdom, Belgium, Luxembourg and France, all had broadband penetration rates higher than the US (22.1%) in July 2007.

[12] http://ec.europa.eu/information_society/policy/ecomm/doc/library/annualreports/13th/com_2008_153_en_final.pdf



Similar figures are revealed by ITU[13]:

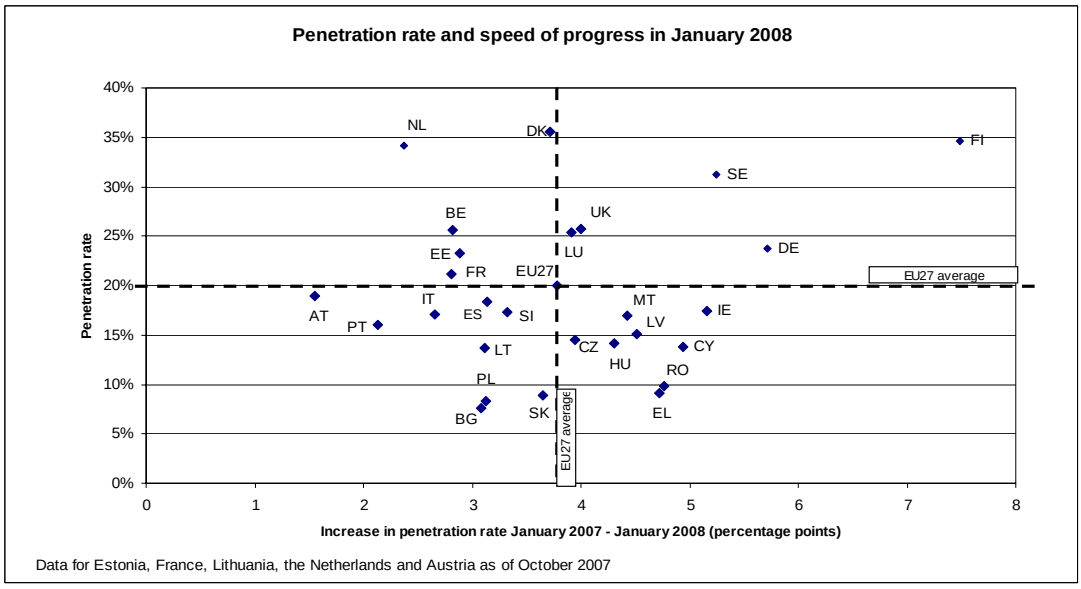
Total broadband Internet subscribers per 100 inhabitants

Rank	Country	Score
1	Denmark	31.74
2	Netherlands	31.72
4	Switzerland	29.47
6	Norway	27.54
7	Finland	27.14
8	Sweden	25.87
11	United Kingdom	21.71
12	France	20.91
15	Luxembourg	19.80
19	Belgium	19.13
21	Austria	17.41
22	Estonia	17.22
23	Germany	17.03
24	Spain	15.34
25	Italy	14.86
27	Portugal	13.85
28	Slovenia	13.41
29	Ireland	12.29
31	Lithuania	10.79
32	Czech Republic	10.64
33	Malta	10.44

[13] Global Information Technology Report 2007-2008, Data source: International Telecommunication Union, World Telecommunication Indicators 2007

34	Hungary	9.70
35	Romania	8.18
36	Poland	6.86
38	Cyprus	5.87
39	Slovak Republic	5.87
41	Croatia	5.53
44	Bulgaria	5.01
45	Latvia	4.78
46	Greece	4.38
49	Turkey	3.74
57	Macedonia, FYR	1.79

EU growth has been highest in Finland, Germany, Sweden, Ireland and Cyprus. Whereas for Finland and Sweden the growth figure follows on from an already advanced position, for the three other counties this represents a 'catching-up'.



In 2007, 77% of all businesses had a broadband connection (97% of large enterprises and 77% of SMEs).

Share of enterprises having a broadband connection					
	2003	**2004**	**2005**	**2006**	**2007**
EU (27 countries)	:	46	62	73	77
EU (25 countries)	:	48	63	74	79
EU (15 countries)	40	50	65	77	82
Euro area	41	49	64	77	82

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

On a global level, in 2005, the International Telecommunication Union estimated 216 708 600 "fixed" broadband Internet subscribers in the world[14].

d. Fixed/mobile telephone lines

The telecoms sector is the biggest single component of the ICT sector, representing about 44% of its market value[15] and 2% of GDP[16]. In 2007, the telecommunication services market was estimated at roughly €300 billion with nominal growth slowing down to 1.9%[17].

Number of main telephone lines per 100 inhabitants					
geo	**2002**	**2003**	**2004**	**2005**	**2006**
EU (27 countries)	48	47	48	47	47
EU (25 countries)	50	49	49	49	49
EU (15 countries)	53	52	52	52	53

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

EU countries rank high on global level in terms of penetration of telephone lines per capita:

Main telephone lines per 100 inhabitants

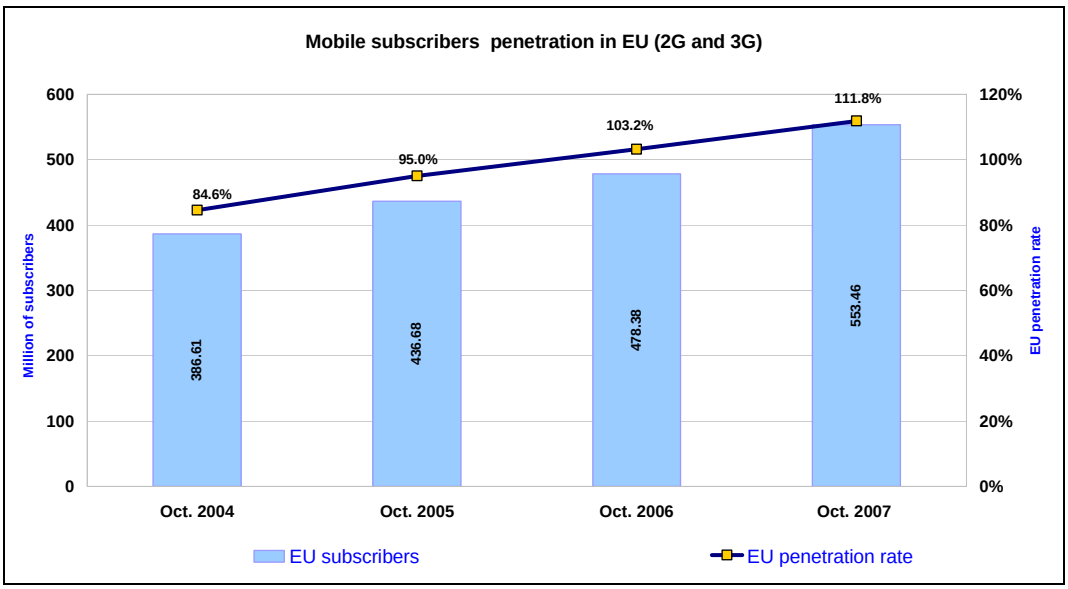
Rank	Country	Score
2	Germany	65.53
6	Sweden	59.52
8	Denmark	56.89
9	United Kingdom	56.15
11	France	55.82
12	Greece	55.52
14	Luxembourg	52.40
15	Malta	50.16
17	Ireland	49.81
19	Cyprus	48.35
20	Netherlands	46.63
21	Belgium	45.21
24	Austria	43.44
25	Italy	43.12
28	Slovenia	42.60
29	Spain	42.38
31	Estonia	40.90

[14] International Telecommunications Union (ITU) (2007) p. 23.
[15] EITO, 2007.
[16] Estimate based on Eurostat figures.
[17] EITO, 2007 Update.

33	Portugal	40.12
34	Finland	36.49
35	Hungary	33.27
36	Czech Republic	31.48
37	Bulgaria	31.28
39	Poland	29.81
40	Latvia	28.64
56	Lithuania	23.19
57	Slovak Republic	21.62
62	Romania	19.44

Source:Global Information Technology Report 2007-2008 (data based on: International Telecommunication Union, World Telecommunication Indicators 2007)

Mobile penetration is even higher. In 2007 it reached 111.8 % of the population compared to 103.2 % the previous year[18]:



Mobile telephone subscribers per 100 inhabitants[19]

Rank	Country	Score
1	Luxembourg	151.61
2	Lithuania	138.06
5	Estonia	125.19
6	Italy	123.08
9	Czech Republic	119.01
11	United Kingdom	116.39
12	Portugal	115.95

[18] COM(2008) 153 final

[19] Global Information Technology Report 2007-2008 (data based on: International Telecommunication Union, World Telecommunication Indicators 2007)

13	Austria	112.80
14	Ireland	111.40
19	Finland	107.76
20	Bulgaria	107.59
21	Denmark	107.25
23	Spain	106.39
24	Sweden	105.92
28	Germany	101.92
29	Greece	99.62
30	Hungary	98.95
32	Netherlands	97.15
34	Poland	95.45
35	Latvia	95.13
36	Slovenia	92.56
37	Belgium	92.55
38	Cyprus	92.06
39	Slovak Republic	90.60
42	Malta	85.96
43	France	85.08
48	Romania	80.45

According to DigiWorld Yearbook 2008, the mobile subscriber base in Western Europe, residential and business combined, reached 438.4 million users at the end of 2006, which represents an increase of 8.2% over the previous year.

e. Online services/activities

- eCommerce/eBusiness

The increase in Internet connectivity and broadbad penetration gave impetus to the wider use of online services. In the period 2004-2007 the share of turnover coming from e-commerce has increased twofold, according to Eurostat survey figures.

E-Commerce via Internet - Percentage of enterprises' total turnover from e-commerce via Internet				
geo	**2004**	**2005**	**2006**	**2007**
EU (27 countries)	2.1	2.7	4.0	4.2
EU (25 countries)	2.1	2.7	4.1	4.2

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

In addition, 15% of all enterprises in the 27 EU MSs have received orders online.

Share of enterprises having received orders on-line					
geo	**2003**	**2004**	**2005**	**2006**	**2007**
EU (27 countries)	:	13	12	14	15
EU (25 countries)	:	14	12	15	16
EU (15 countries)	9	15	13	16	17
Euro area	7	12	10	12	15

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

Another survey[20] estimates that in the period 2007-2010 the online sales will almost double for Western European countries, whereas for CEE countries the increase will be more than two times, reaching a total of 261.3 billion EUR.

Online retails sales forecast by country

Billion EUR		**2006**	**2007**	**2008**	**2010**
Western Europe	Total	88.2	123.9	168.6	**221.3**
	France	12.7	17.4	23.5	32.7
	Germany	19.0	27.6	37.4	51.3
	Italy	3.8	6.2	9.1	12.5
	Spain	4.0	5.3	10.3	19.4
	United Kingdom	30.2	37.6	45.7	52.2
	Rest of Europe (NL, BE, LU, NO, SW, DK, FI, AU, CH, IR, PT, GR)	18.5	29.8	42.6	53.2
North America	USA	84.5	95.6	114.0	140.0
Asia-Pacific	China	14.0	29.4	56.0	181.4
	Japan	30.0	37.5	45.0	62.8
Rest of the World	CEE	16.0	18.4	25.0	**40.0**
	Latin America	14.0	22.4	32.0	70.0
	Africa and Middle east	8.0	10.4	14.0	24.0
Total		254.7	337.6	454.6	739.5

At the same time the percentage of individual purchasing online has been increasing. More than one-fifth of the EU citizens were buying online by the end of 2007.

Percentage of individuals who ordered goods or services, over the Internet, for private use, in the last 3 months				
	2004	**2005**	**2006**	**2007**
***eu27* European Union (27 countries)**	15	18	20	23
***eu25* European Union (25 countries)**	16	18	21	24
***eu15* European Union (15 countries)**	21	21	23	27

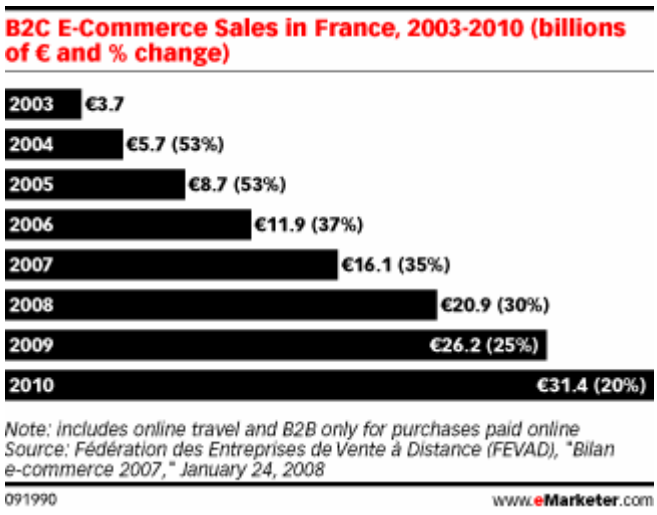
Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

[20] DigiWorld Yearbook 2008, The Digital World's Challenges

According to EIAA Online Shoppers[21], 80% of European Internet Users bought a product or service online in 2007, up 3% since 2006 and double the 2004 figure. These European online shoppers made 1.3 billion purchases in just a six month period, spending an average of €747 each online. In addition, the study observes that the European online shoppers are heavy users of the Internet. 84% of online shoppers go online via a broadband connection and on average they use the Internet on 5.7 days each week, spending an average of 12.3 hours online (above the European average of 11.9) and over half (51%) log onto the Internet every day.

The Internet is also increasingly popular for C2C sales. In 2006, more than 170.000 Europeans were living off the income they generate from selling goods on eBay. This thriving market is enabling the creation of thousands of micro enterprises. According to FEVAD, by the end of 2006, 64% of Internet users in France had bought or sold items trough a site that offers consumer-to consumer sales platform.

French trade group FEVAD (fevad.com) predicts that B2C e-commerce in France will grow 30% in 2008. That is down from 35% growth rate in 2007, but still quite healthy[22].



French consumers have a generally high opinion of online buying. More than 85% of French respondents to a Benchmark/Brandalley (http://www.brandalley.fr/) survey revealed that online retailers offered better prices and reductions than offline stores. More than one-half also said online shopping helped them avoid crowds.

A survey by DirectPanel in May 2008[23] found that over half of the 12,000 French shoppers polled had bought books, CDs, DVDs, software, train or plane tickets online. One-half had also bought clothing and shoes or other leather goods, which are typically hard to sell online. All these purchases indicate a major commitment to online shopping.

Germany is also a steady market, thanks to its large population as well as the efficiencies of major online retailers. eMarketer[24] estimates that more than three-quarters of the German Internet users are already buying online, and this percentage

21 http://www.eiaa.net/news/eiaa-articles-details.asp?id=158&lang=1
22 http://www.emarketer.com/Article.aspx?id=1006355
23 http://www.directpanel.com/info/ecom08/CP_DirectPanel_eCom2008.pdf
24 http://www.emarketer.com/Article.aspx?id=1006355

should continue to rise. Nielsen (http://nielse-online.com/) estimates the number even higher – 97%.

B2C E-Commerce: Germany, 2006-2011

	2006	2007	2008	2009	2010	2011
B2C e-commerce sales* (billions)						
Dollars	$27.1	$38.8	$50.5	$60.1	$69.4	$79.6
€	€21.5	€28.5	€36.6	€45.5	€54.2	€63.6
% change (based on € figures)	-	32.6%	28.4%	24.3%	19.1%	16.6%
Online buyers (millions)						
Internet users ages 14+	36.6	39.1	41.5	43.9	46.3	48.5
Online buyers ages 14+	27.2	29.2	31.3	33.4	35.4	37.3
% change	-	7.5%	7.0%	6.6%	6.2%	5.4%
% of Internet users who are online buyers	74.2%	74.9%	75.4%	76.0%	76.5%	77.0%
Average annual amount spent online per buyer**						
Dollars	$996	$1,326	$1,614	$1,801	$1,959	$2,133
€	€790	€975	€1,170	€1,364	€1,530	€1,693
% change (based on € figures)	-	23.3%	20.0%	16.6%	12.2%	10.6%

*Note: converted at average annual exchange rates (projected for future years); *includes online travel, event ticket and digital download sales; **individuals ages 14+ who have made at least one purchase online within the past year*
Source: eMarketer, July 2007

085639 www.eMarketer.com

One of the reasons e-commerce is expected to remain strong in Europe is that online buying has reached critical mass and is being adopted by very large numbers of Europeans in a variety of categories. Eurostat figures for 2006 reveal that 12% (compared to 9% in 2005) of the individuals who, in the last 12 months, haven't ordered goods or services over the Internet, did not do it because they were worried about giving credit card or personal details over the Internet. Only 1% pointed as a reason the slow speed of the Internet connection.

Consumer confidence can easily be destroyed if the availability and reliability of the provided services is not maintained. Therefore, secure and always on networks are needed in order to ensure that consumers continue to exploit the benefits of e-commerce and that businesses are able to profit from greater customer reach and improved efficiency.

- eBanking

Online banking is yet another service for which secure and reliable Internet is of crucial importance. In 2007, almost 80% of enterprises were making use of e-banking, compared to 70% in 2005 (Eurostat).

- eGovernment

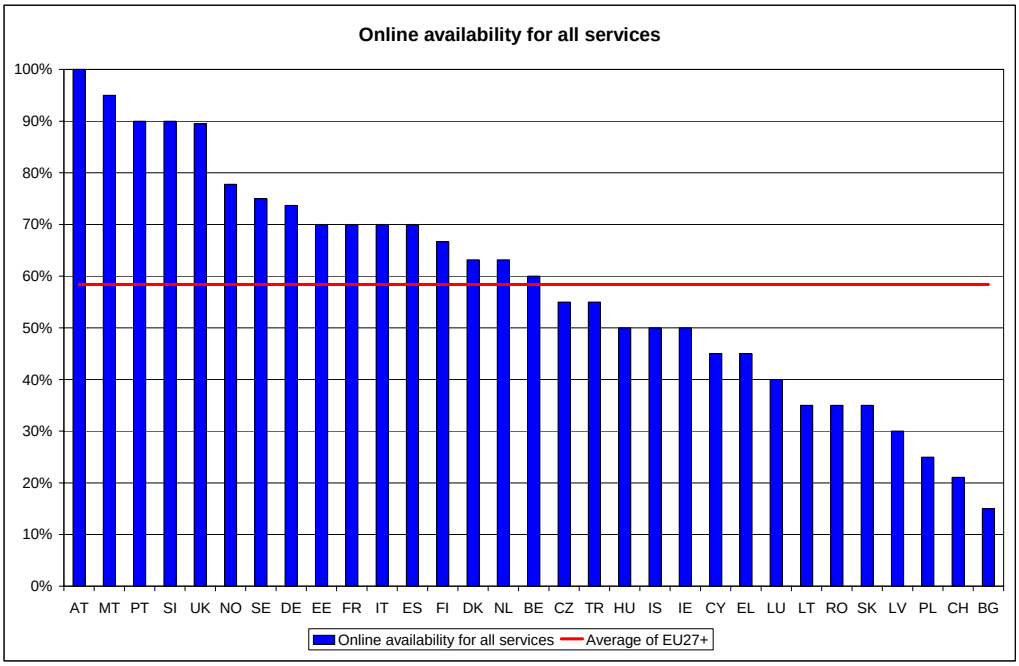
In recent years Europe has continued making progress in the supply of online public services thus making progressing towards the goals of the Lisbon Strategy and the i2010 eGovernment action plan.

E-government availability					
geo	2002	2003	2004	2006	2007
EU (27 countries)	:	:	:	:	59
EU (25 countries)	:	:	41	51	:
EU (15 countries)	36	47	49	56	:

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

The availability of e-government services has been steadily increasing. In 2007, 59% of the services measured were fully available i.e. the full transaction could be carried out online. This is up from around 50% in 2006 and represents the largest percentage increase for a single year.

Basic services[25] in all Member States are available online, and there has been a significant increase in the level of sophistication. However, the gap between the leading Member State – Austria, now with 100% fully available - and the worst performer is 85 percentage points. This is an important fact to be taken into account as the countries where availability of eGovernment services is not so high, might take a more "relaxed approach" to security and resilience issues.



Source: Cap Gemini, "The User Challenge. Benchmarking the supply of online public services" 2007

eGovernment is still progressing faster for business services than for services intended for citizens. The EU average for company registration fully available online, a good indicator for a business-friendly environment and crucial to the Lisbon agenda, is 79%.[26]

[25] Basic refers to the 20 services (12 for citizens, 8 for businesses) used to benchmark online availability of public services (full definition in "The User Challenge" Report, see next footnote)

[26] SEC(2008) 470

There is a strong correlation between the **sophistication** and availability of eGovernment services. Five countries achieve 90% or above on both measures. Austria retains its leading position, followed by Malta, Slovenia, Portugal and the United Kingdom (the first of the large countries). Modest size has enabled rapid progress. However, a number of small Member States have not yet embraced eGovernment to the same degree. There are also a number of previously progressive 'old' countries whose progress has faltered somewhat over recent years.

Nearly half of individuals and 61% of businesses have used eGovernment to obtain information. Where sophistication is concerned, nearly 22% of citizens were able to fill in forms online, up 10 percentage points since 2005, compared with 46% of businesses.

eGovernment is still progressing faster for business services than for services intended for citizens. The EU average for company registration fully available online, a good indicator for a business-friendly environment and crucial to the Lisbon agenda, is 79%. It is 100% in fifteen Member States, but in seven others (FI, NL, EL, BG, RO, LV, SK) it remains only at 50%. VAT and corporate tax declaration are both close to 100%, while the EU average for electronic procurement is 81%.

The situation is different for citizens. Sophistication stands at 70% and full online availability for services at 50%. The gap between the leader (Austria — 100%) and the worst performer exceeds 90 percentage points, although in some countries (UK, FI, NO, SI) citizens are now served as well as businesses.

According to the Community surveys on ICT use in businesses and households, 2007 saw a significant improvement in the **take-up** of eGovernment services, both by individuals and businesses. For individuals, 30% of Internet users have interacted online with public authorities in one way or another. This represents a 6 percentage point increase relative to 2006, but still lags behind the figure for businesses (66%). However, the development is very encouraging, and is likely to signal a positive trend after years of slow growth in take-up.

E-government usage by individuals - Percentage of individuals who have used the Internet, in the last 3 months, for interaction with public authorities

geo	2005	2006	2007
EU (27 countries)	23	24	30
EU (25 countries)	23	26	32
EU (15 countries)	26	:	34
Euro area	25	27	33

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

E-government usage by enterprises - Percentage of enterprises which use the Internet for interaction with public authorities				
geo	**2004**	**2005**	**2006**	**2007**
EU (27 countries)	51	57	63	65
EU (25 countries)	52	57	64	67
EU (15 countries)	50	56	64	66
Euro area	51	58	65	68

Source: Eurostat, Science and Technology theme, Information Society, http://epp.eurostat.ec.europa.eu

The Global Information Technology Report 2007-2008 also shows very high availability of government online services:

In your country online government services such as personal tax car registrations passport applications business permits and e-procurement are (1 = not available 7 = extensively available)

Rank	Country	Score
1	Estonia	6.48
3	Denmark	6.13
4	Sweden	5.90
5	Ireland	5.82
6	Malta	5.79
8	Austria	5.72
11	Norway	5.67
14	United Kingdom	5.54
17	Finland	5.38
20	France	5.22
24	Netherlands	5.15
26	Portugal	5.12
31	Germany	4.60
32	Spain	4.58
33	Belgium	4.53
34	Lithuania	4.51
35	Slovenia	4.46
38	Luxembourg	4.37
46	Cyprus	4.11
48	Hungary	4.09
57	Bulgaria	3.75
58	Italy	3.73
68	Greece	3.37
73	Romania	3.29
74	Latvia	3.28
79	Slovak Republic	3.15
84	Czech Republic	3.07
91	Poland	2.87

- **eVoting**

Electronic voting (also known as e-voting) encompasses several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting technology can include punch cards, optical scan voting systems and specialized voting kiosks. It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet (i-voting).

At least 13 EU countries have tested or implemented e-voting projects, according to the Competence Center for Electronic Voting and Participation[27], which provides examples of such projects for the following countries: Austria, Belgium, Bulgaria, Estonia, Finland, France, Germany, Italy, Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

Germany started e-voting tests and pilots already in 1999[28], and is continuing them, only at non-political/parliamentary elections, like at universities - students' bodies elections (Osnabrück, Bremerhaven) -, at local advisory level - youth community and senior citizens councils - as well at public and private employees councils. In Great Britain, many different electronic voting methods have been experimented since 2002, for example, polling booth, telephone, SMS, remote electronic voting via Internet and digital television. Remote electronic voting systems were used in the local election in 30 municipals in 2003 when 27% of the votes were cast electronically (146 000 votes).

All French expatriates residing in the USA were given the possibility to validly elect via the Internet their representatives to the French "High Council of French Citizens Abroad", a public law body designating 12 members of the Upper House of Parliament (*Sénat*), in May 2003. This was well taken up and led, amongst other consequences, to a marked reduction of work by French consulates on election day - more than half of the votes were cast electronically in any district - but not to a general rise in participation. Spain, started testing e-voting in polling stations, kiosks and via the Internet, in 2002, *inter alia*, through a 'body salinity identification'. An i-voting test for Catalonians abroad, in parallel to the November 2003 election to the regional parliament was conducted in Argentina, Belgium, Chile, Mexico and the USA. Furthermore, on 14 March 2004, on the occasion of parliamentary elections, voters of three municipalities (Lugo (Mosteiro-Pol), Zamora and Toro (Zamora)) were given the possibility to test i-voting with smart cards after having cast their votes at a polling station.

The Netherlands – besides its traditional e-voting at polling stations – decided to run valid pilots on i-voting and telephone voting at the EP elections of mid-June 2004, also from abroad, while e-voting at polling stations would be eased. Italy and France have been testing an e-voting system in polling and police stations on small scale, with smart cards and fingerprint recognition, and which will be tested again in both countries at the EP elections of 2004 where the elector can choose to vote for the MEPs of the country of residence or of citizenship. From a technical point of view, this method could also be used on private Internet computers.

In Austria, a first test of remote e-voting by the Internet was undertaken *in parallel* to the elections of the *Austrian Federation of Students*, in May 2003, at an institute of the

[27] http://db.e-voting.cc/europe

[28] The examples are based on: Buchsbaum, Thomas M., "E-Voting: International Developments and Lessons Learnt" http://www.e-voting.cc/static/evoting/files/buchsbaum_p31-42.pdf

Vienna University of Economics and Business Administration, by a team of scientists led by Alexander Prosser, of Vienna University of Economics and Business Administration, which had developed the e-voting system used, itself.

Estonia has advanced the farthest in deploying Internet voting. Since 2000, it has conducted two national elections in which all voters could use Internet voting. The first election, in October 2005, was for local offices and the second election, in March 2007, was a national parliamentary election. A public opinion poll said that general support to e-voting is 73% of voting age inhabitants, but the real result was 1.8% e-votes of all votes. There were not successful attacks against the e-voting system. The target group of the e-voting system was 1 million voters.[29]

Main Statistics of eVoting (Internet Voting at the Elections of Local Government Councils on October 2005)[30]

	ELECTIONS TO THE LOCAL GOVERNMENT COUNCILS 2005	PARLIAMENTARY ELECTIONS 2007
Number of eligible voters	1 059 292	897 243
Voter turnout	47.4 %	61.9 %
Votes:	502 504	555 463
valid	496 336	550 213
invalid	6 168	5 250
E-votes given	9 681	31 064
incl. repeated e-votes	364	789
Number of e-voters	9 317	30 275
E-votes counted	9 287	30 243
E-votes cancelled by paper voting	30	32
Percentage of e-votes among all votes given	1.9 %	5.4 %
Advance votes (e-votes included)	129 329	171 518
% of e-votes among advance votes	7.2 %	17.6 %
Percentage of e-voters who used ID card electronically for the first time	61 %	39 %

As e-voting slowly but surely is gaining popularity, security experts are concerned about the problems associated with it. Electronic-voting machines remain vulnerable to

[29] Triinu Mägi, Practical Security Analysis of E-voting Systems, 2007

[30] http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf

attacks from people trying to steal election vote and to glitches that incorrectly count votes. The greatest worries of security experts are not related to malicious attacks against e-voting servers, but the system and programming errors and the security of private computers. Another complicated problem seems to be the contradicting properties of correctness and privacy harmony.[31]

- eWorking (Teleworking)

Telework is a developing trend and offers benefits to both workers and employers. It is both a way for companies and public service organisations to modernise work organisation, and a way for workers to reconcile work and social life and giving them greater autonomy in the accomplishment of their tasks.

Telework is a form of organising and/or performing work, using information technology, in the context of an employment contract/relationship, where work, which could also be performed at the employers' premises, is carried out away from those premises on a regular basis[32].

In 2002 an European Framework Agreement on telework, concluded between the social partners at European level (ETUC (and the liaison committeeEUROCADRES/CEC), UNICE/UEAPME and CEEP), was signed in July 2002 and was subsequently due to be transposed to the Member States in accordance with the procedures and practices of the social partners at national level.

The number of teleworkers concerned by the agreement, was estimated at 4.5 million employees in 2002. There are no comparable cross-border data to measure its development since then. It is generally considered that telework is more widespread in some sectors of activity, such as in telecommunications, and for qualified workers. Moreover, the importance of telework varies greatly from one country to another. Some estimates indicate a rate close to 8% of the working population in the Netherlands or the UK, around 5% in Spain, Germany and France and just above 2% in the Czech Republic or Hungary. [33]

A study done by the Institute for Employment Studies in the UK[34] concluded that there were over 9 million eWorkers in Europe in 2000. As can be seen in Table X, the largest single group were multilocational eWorkers, estimated at 3.7 million. This group includes employees who work partly at home and partly in the office, as well as those who work nomadically or from clients' premises.

[31] Triinu Mägi, Practical Security Analysis of E-voting Systems, 2007
[32] Framework agreement on telework - July 2002
[33] http://ec.europa.eu/employment_social/news/2006/oct/telework_implementation_report_en.pdf
[34] Modelling eWork in Europe: Estimates, models and forecasts from the EMERGENCE project, Bates P, Huws U. Report

Estimates of telehomeworkers, eEnabled workers and eEnhanced workers in Europe, 2000

		EU 15
1.	**Home-based employees** who use a computer and telecommunications link to conduct their work (person equivalent)	810,000
2.	**Multilocational employees** who use a computer and telecommunications link to conduct their work (person equivalent)	3,700,000
3.	**eLancers** providing business and related industries who use a computer and telecommunications link to conduct their work	1,450,000
	Number of person equivalent eWorkers: sum of 1-3 above	**5,960,000**
4.	Number of **eEnabled self- employed** workers who require a computer and telecommunications link to conduct their work not working in business related industries	3,080,000
	Number of person equivalent eWorkers: sum of 1-4 above	**9,040,000**
	Estimated number of eWorkers based on CLFS and UK LFS (including irregular eWorkers)	**9,830,000**

Source: EMERGENCE analysis, 2001

Employees who work exclusively from their homes using ICTs (often presented in the media as the archetypal teleworkers) are in fact rather rare, comprising only an estimated 810,000 in the EU workforce in 2000.

However, there were, an estimated 1.45 million ‘elancers’ supplying business services to clients using ICTs and a further over 3 million self-employed people whose home-based businesses are dependent on ICTs (the so-called ‘eEnabled self-employed’). This makes a combined total of some four and a half million self-employed teleworkers across Europe, forming approximately half of the total number of teleworkers.

The same study further attempted to develop estimates to 2010. According to the forecast, if current employment trends continue, approximately a million new eWorkers are likely to appear over the ten-year period. However, if technological and organisational change continue at current rates, there is likely to be considerable growth in eWork which, combined with the effects of employment growth, will effectively triple the numbers, to reach 27.12 million by 2010.

By far the largest part of this growth is to involve multilocational eWorking by employees, forecast to top 14.3 million. This is followed by eEnabled self-employment, which is predicted to grow to 6.6 million. This form is likely to grow more slowly and reach a plateau sometime after 2010.

Projections of the telehomeworkers, multilocational eWorkers and eLancers, 2010

	Employment growth	ICT diffusion	Employment growth and ICT diffusion
Telehomeworking employees	950,000	2,750,000	3,170,000
Multilocational eWorkers (person equivalent)	4,310,000	12,463,000	14,332,000
eLancers (providing business related services)	1,790,000	2,490,000	3,040,000
eEnabled self-employed	3,080,000	6,580,000	6,580,000
Total estimate of individualised eWorking	**10,130,000**	**24,283,000**	**27,122,000**

Source: EMERGENCE analysis, 2001

The leading teleworking country in Europe, according to the results of a survey which was commissioned by the EU, is Finland[35]. As per the survey, **16.8%** of the labour force in Finland consists of teleworkers, the closest runner-up being Sweden with 15.2 per cent, followed by Holland with 14.5% and Denmark with 10.5%. The estimated potential of teleworking in Finland, ie the amount of work that could be transferred, at least partially, into this method of working, varies from 20 to 40 per cent in the different sectors of industry. The conclusion is obvious: teleworking is here to stay, it has become more common - according to Finnish research it has increased fivefold during the last decade - and it will continue to expand.

In the UK, work patterns also appear to be undergoing technology-driven changes. From questions asked in its labour force survey, the Office for National Statistics found that in Spring 2005, 2.1 million people in the United Kingdom working mainly from home (or using home as a base) were only able to do so because they used **both** a telephone **and** a computer. The proportion of the workforce who tele-worked using both a telephone and a computer rose from 3% of the total workforce in 1997 to 7% in 2005 (ONS, 2005)[36].

- eHealth

ICTs can have a huge impact on all aspects of healthcare, from delivering the information people need to lead a healthy lifestyle to providing new tools to design new medicines; from making healthcare systems more efficient and responsive to providing 'in the home' and mobile healthcare technologies.

eHealth means Information and Communication Technologies tools and services for health. eHealth covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals. Examples include health information networks, electronic health records, telemedicine services, wearable and portable systems which communicate, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring and lifestyle management. [37]

[35] http://netti.sak.fi/sak/englanti/articles/teleworking.htm

[36] OECD, Measuring the Impacts if ICT Using Official Statistics, http://www.oecd.org/dataoecd/43/25/39869939.pdf

[37] http://ec.europa.eu/information_society/activities/health/whatis_ehealth/index_en.htm

A pan-European survey on electronic services in healthcare ("Benchmarking ICT use among General Practitioners in Europe") published by the European Commission in 2008 shows a growing role of eHealth applications in the doctor's practices. According to it, 87% of European doctors (General Practitioners) use a computer, 70% of European doctors use the Internet and 48% have a broadband connection. European doctors increasingly store and send patients' data such as lab reports electronically. In using such eHealth applications, doctors and medical services have already improved healthcare in Europe through, for example, more efficient administration and shorter waiting times for patients. The report also highlights where doctors could make better use of ICT to offer services such as telemonitoring, electronic prescriptions and cross border medical services.[38]

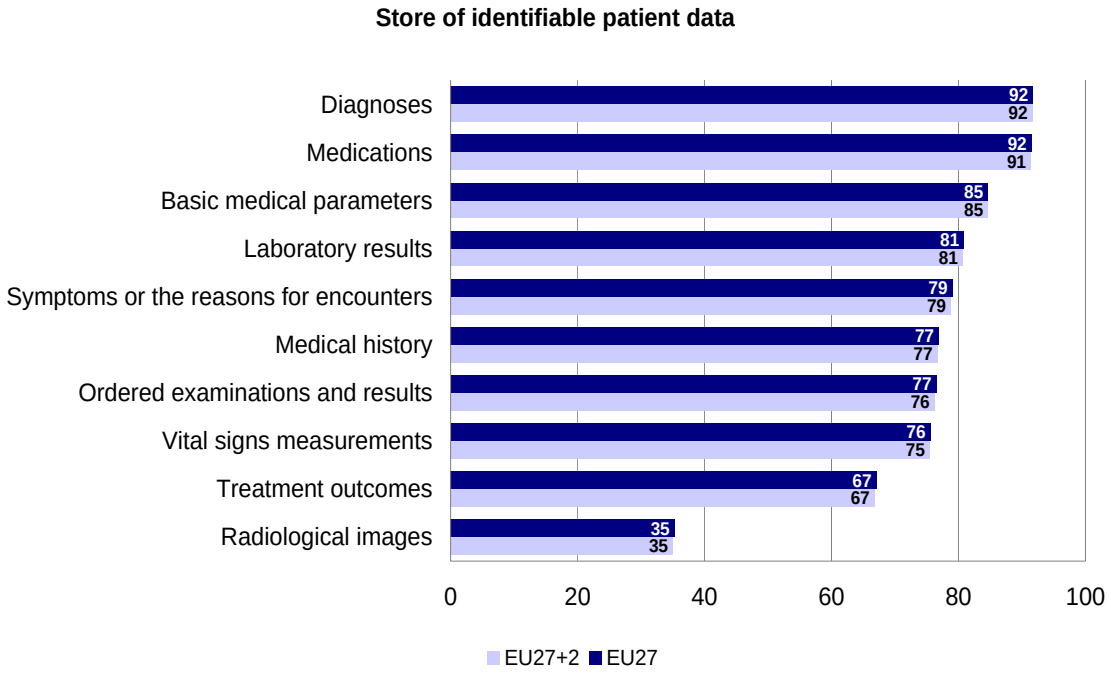
	Use of computers in European general practices				Use of broadband in European general practices			
	Single GP	2-3 GPs or physicians	4+ GPs or physicians	Total	Single GP	2-3 GPs or physicians	4+ GPs or physicians	Total
EU27	83.8	90.6	92.6	87.4	41.1	53.4	59.1	47.9
EU27+2	83.8	90.7	92.8	87.5	41.1	53.7	59.7	48.1
BE	80.8	96.4	96	86.1	74.9	88.7	88.1	79.5
BG	95.3	100.0	100	97.1	25.0	17.9	30.0	23.0
CZ	81.7	85	85	82.2	37.2	46.9	45.5	38.5
DK	96.9	100.0	100.0	98.9	86.8	93.8	93.3	91.0
DE	99.4	97.6	100	98.8	38.0	39.5	80.0	40.0
EE	100	100	100.0	100.0	59.4	76.0	84.0	72.0
EL	74.2	96	96.1	79.4	38.2	61.9	66.7	43.8
ES	68.2	74.3	87.1	77.2	21.3	49.2	42.5	35.8
FR	78.3	89.4	100	82.8	54.9	67.0	55.6	59.1
IE	58.5	88.4	100	73.4	28.9	61.3	81.3	44.3
IT	82.6	95	98	86.2	46.2	47.2	64.1	48.8
CY	74	100	56	69.4	35.7	25.0	26.1	31.9
LV	90.0	83	87	88.1	58.8	62.1	33.3	58.3
LT	61	60.3	56.5	57.4	15.0	29.8	36.6	32.7
LU	75	95	67	79.7	54.1	84.3	33.6	61.5
HU	100.0	100	100	100.0	38.6	41.9	16.7	35.7
MT	71	33	63	65.2	52.1	25.0	52.0	50.6
NL	96.2	99.1	100.0	98.5	82.7	82.3	80.0	81.6
AT	77.3	91	98.6	83.6	27.9	46.7	71.1	36.8
PL	61.3	75.9	78.7	71.5	29.2	28.8	38.7	32.1
PT	55.4	92.2	100.0	88.0	13.8	32.5	43.5	32.1
RO	71.3	56.4	60	65.8	6.0	4.2	4.5	5.3
SI	100	78	98.5	97.1	59.3	44.4	52.9	54.0
SK	95.5	96	97	95.8	16.0	13.0	13.3	15.3

[38] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/641&format=HTML&aged=0&language=EN&guiLanguage=en

FI	100	100	100.0	100.0	80.0	91.7	94.6	92.7
SE	96	100	100.0	99.6	78.3	81.3	91.9	88.1
UK	87	100.0	100.0	97.3	46.4	79.7	76.1	72.6
IS	100	94	100.0	99.0	83.3	83.3	87.0	85.7
NO	83	100.0	100.0	98.0	34.8	75.9	83.5	73.8

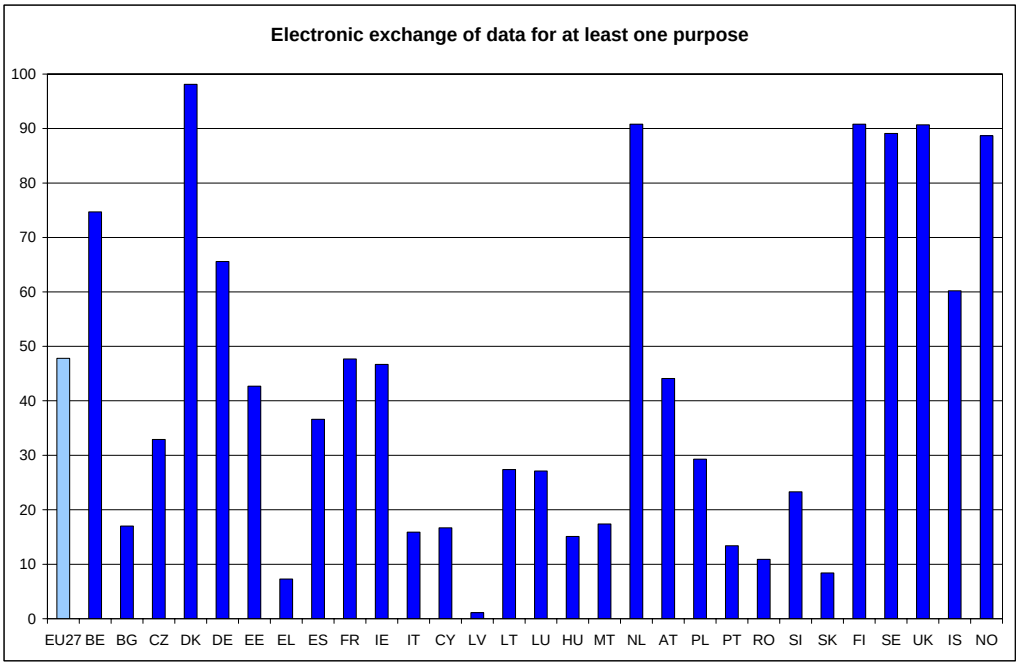
Source: Empirica, Pilot on eHealth Indicators, 2007

Administrative patient data is electronically stored in 80% of general practices: 92% of these also electronically store medical data on diagnoses and medication; 35% electronically store radiological images. European doctors often transfer data electronically with laboratories (40%), and occasionally with other health centres (10%).



Source: Empirica, Pilot on eHealth Indicators, 2007

The countries most advanced in ICT access and connectivity are more likely to use them for professional purposes. For example, Denmark, where high-speed Internet is most widely available in Europe, sees extensive use of email communication between doctors and patients in about 60% of practices (the EU average is only 4%).



Source: Empirica, "ICT use among General Practitioners in Europe" 2008

Electronic prescriptions (e-Prescribing), which is practiced by 6% of EU General Practitioners, and in some Member States it is widely used: Denmark (97%), the Netherlands (71%) and Sweden (81%).

Exchange of patient data across borders is still low (only 1% of the EU's General Practitioners), however the European Commission aims to promote cross-border interoperability of electronic health record systems and is planning to launch, with several countries, a project on cross-border eHealth services for patients traveling within the EU.

The provision of eHealth services is dependent on the security of the networks over which information is exchanged, given the sensitivity and the importance of the transferred data.

2. TYPES AND IMPACT OF CYBER-ATTACKS

a. Types of cost/impact

The costs associated with cyber-attacks can be seen as *direct* and *indirect* costs[39].

Direct costs include:

- the expenses incurred in restoring a computer system to its original, pre-attack state. Recovery from an attack usually requires extra spending on labor and materials, i.e. increased spending on IT security, accelerated upgrade in hardware or software is after an attack.

[39] The classification is based on: Cashell, Jackson, Jickling, Webel, "The Economic Impact of Cyber-Attacks"

- another set of direct costs arises from business interruption. These costs may include lost revenue and loss of worker productivity during the disruption. Lost sales may be a transitory phenomenon, limited to the attack period (and possibly made up afterwards), or they may be long-term, if, for example, some customers switch permanently to competing firms.

- Another direct cost may involve the loss of value in information assets that are stolen, compromised, or otherwise degraded during an attack. The value of an information asset is highly dependent upon who possesses the information. Sensitive commercial R&D information in the hands of a competitor is significantly more problematic than if it were in the hands of a Netherlands teenager. Time sensitivity can also complicate the valuation problem. For example, a password that expires in ten seconds is worthless after it has expired, but it is quite valuable during the ten seconds that it could be used to gain system access. Some losses are difficult to quantify, such as the loss of reputation and trust, embarrassment, etc.

Indirect costs

Attacks also have indirect costs, which may continue to accrue after the immediate damage has been repaired. Many indirect costs flow from loss of reputation, or damage to a firm's brand. Customers may defect to competitors, financial markets may raise the firm's cost of capital, insurance costs may rise, and lawsuits may be filed. Some of these cost factors are readily quantifiable, but other aspects of loss of trust or confidence are intangible and difficult to measure.

Indirect costs of cyber-attacks may also include economic harm to individuals and institutions other than the immediate target of an attack. An attack on one firm's computer networks may affect other firms up and down the supply chain. When credit card data is hacked, or an Internet service provider goes down, consumers suffer costs. From an accounting perspective, these do not count as costs to the target firm, but from a policy perspective they can be significant. The possibility of cascade effects – disruption spreading from computer to interlinked computer – is well-known, but we are far from being able to quantify the economic impact of an event of this type.

Another study[40] subdivides financial damage resulting from the interruption of Internet services into four categories:

- **Downtime Loss** The downtime costs can be split further into *productivity loss* (employees can no longer do "business as usual" and have to use less efficient ways to fulfil their duties; certain tasks can only be done later) and *revenue loss* (lost transactions by customers that cannot access a service or due to the inability of a company to fulfil customer requests).
- **Disaster Recovery** Costs of the time that employees and external staff have to spend on recovery from an incident. Additionally, material costs can arise.
- **Liability** Many companies offer service level agreements (SLAs) to their customers. In case that their service quality deviates from an SLA, the customer can claim compensation payments. Liability related losses can be partially insured and typically arise several days after the incident.

[40] Dubendorfer, Wagner, Plattner, "An Economic Damage Model for Large-Scale Internet Attacks"

- **Customer Loss** Customers being dissatisfied by degraded service quality might terminate their contract. The rate of new customers joining a service can substantially drop if the reputation of a company suffers. These opportunity costs arise typically weeks to months after an incident.

One of the findings of the study on business dependence on the Internet[41], made on the example of US businesses, claims that an Internet disruption will affect nearly every US company directly or indirectly, and the efforts to respond will create ***stress points*** that will hinder recovery. In a situation in which the Internet is down or found to be unreliable for an extended period, companies are likely to turn to conventional methods of communication and processing until Internet service can be restored. Where such backup capabilities are possible, their use will put enormous stress on the telecommunications, mail, delivery and office supply industries, and thus success at mitigating the economic impact of a disruption will largely depend on the ability of these industries to successfully manage a surge in demand and sufficiently scale up operations using spare capacity, temporary labor and/or creative work-arounds.

Other stress points from a widespread Internet disruption could include:

- **Demand for cash.** Financial institutions will face a demand for cash if Internet-based delivery channels are perceived as vulnerable or unreliable, potentially creating a need to replace electronic communications with manual, paper-based methods.
- **Temporary workers.** Temporary workers will be in high demand as companies use less-efficient paper systems. Such provisional systems and workers will be unable to sustain the corporate knowledge that central, automated processes have provided.
- **Gasoline and other fuels.** Energy company distribution systems could be hampered by an Internet disruption. At the same time, demand for gasoline could increase vehicle traffic because workers who telecommuted must now go into the office to access private networks.
- **Fuel hoarding** also could occur. Transportation fuel providers may need to enforce rationing and/or physical security measures at fuel stations depending on the nature of the crises and the public response.
- **Unavailability of alternative technology.** Efforts to return to telephone-based communications and faxes to restore company operations will place new demands on equipment that often was being phased out or replaced. Moreover, this equipment may be Internet-dependent in some cases.
- **Paper and other office supplies.** Office supply companies will experience a surge in demand for paper-based methods of communication, and their own supply and distribution operations may be compromised by the disruption.
- **Greater demand on existing phone systems.** Sales and other transactions currently done on the Internet will be replaced by telephones.
- **Congested transportation systems.** Transportation networks are likely to become more congested as delivery services and in-person meetings increase and as work-at-home employees are forced to go into local offices to access private networks.

[41] Growing Business Dependence on the Internet, Business Roundtable, 2007

A study of the Business Roundtable[42] finds that a widespread and sustained Internet disruption will ripple through the economy in several ways that will have a notable significance to business. These include:

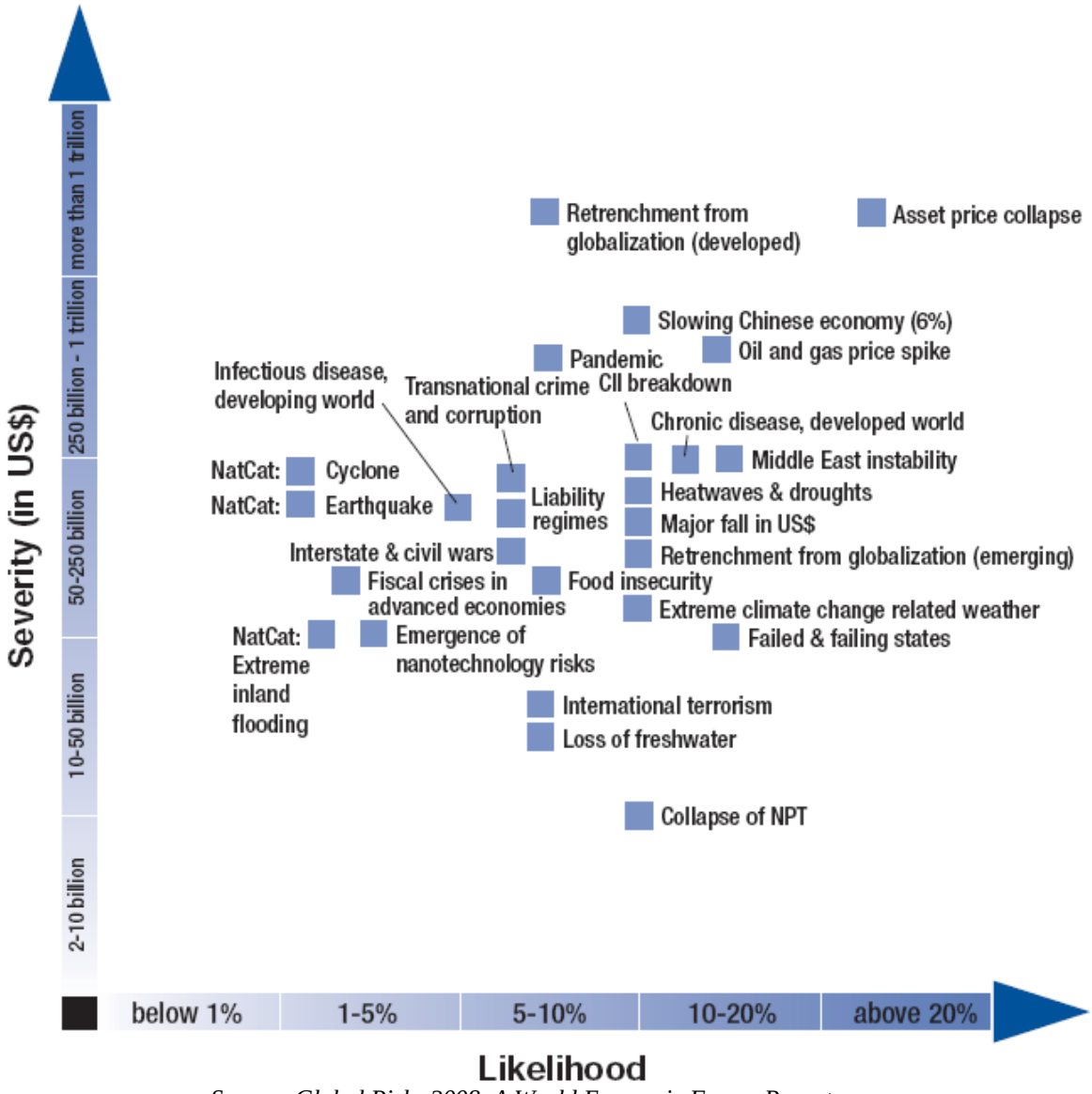
- **Drop in productivity.** An instantaneous drop in productivity will be accompanied by a fall in economic output as processes become less efficient and the workforce is destabilized. A typical Business Roundtable company could experience degraded productivity of as much as $1 million per day.
- **Congestion costs.** Because businesses will no longer have the option of using the Internet for business applications and services, they will replace these services with the next-best options, when available, which will likely be more time consuming and costly. This could lead to new and unexpected "congestion costs" on the economy.
- **Lower profits and stock market declines.** A fall in productivity and subsequent reduction in expected profits will affect the stock market, as stock values will decline to reflect higher costs and lower profits. The reaction of the stock market could be greater if investor confidence is shaken, which would likely be the case in the event of a terrorist attack.
- **Reduced consumer spending.** A decrease in the value of stocks is likely to have a "wealth effect" as consumers will be inclined to reduce their consumption because they feel less wealthy – further depressing demand and output in the economy.
- **Potential liquidity crisis.** Cash could be in short supply if automated payment systems are interfered with due to the Internet disruption, leading to a potential liquidity crisis. This new demand for cash could be exacerbated if more vendors require cash payment because of greater difficulties in determining whether a customer has available credit. If fewer credit sales are authorized, the increasing challenges for cash-constrained households will have a further depressing effect on the U.S. economy.

While the costs associated with lost productivity and the wealth effect can be significant, the costs of congestion and potential large-scale infrastructure failures could be even larger due to the cascading effects of a widespread and sustained Internet disruption across the economy.

b. Likelihood of a major Internet disruption

According to the World Economic Forum, a breakdown of the CII is one of the core risks facing the international economy. The World Economic Forum estimates that there is a 10 to 20% probability of a CII breakdown in the next 10 years, one of the highest likelihood estimates of the 23 global risks it examined in a recent report. The report estimates the global economic cost of the incident at approximately $250 billion, or more costly than two-thirds of the risks.

[42] BR, Internet Business Dependence Report, 2007

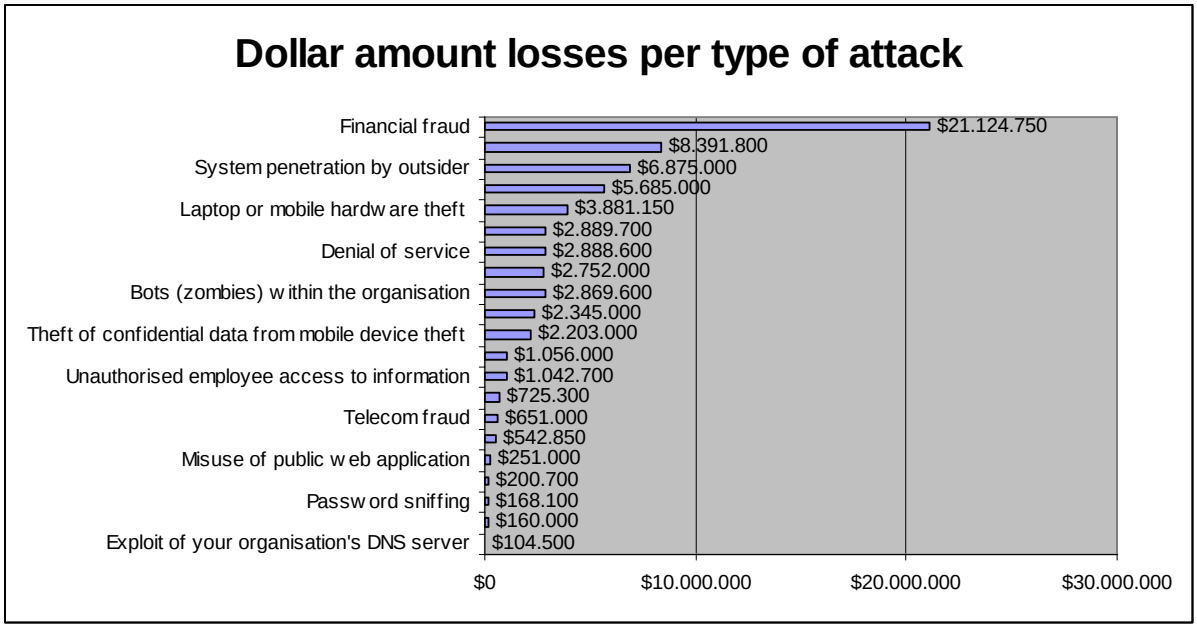


Source: Global Risks 2008, A World Economic Forum Report

c. Types of threats

The CSI Survey 2007[43] shows the amounts of losses expressed in USD suffered by its respondents per different types of attacks. Respondents' estimates of the losses caused by various types of computer security incident were up substantially in comparison to 2006 even though the number of respondents who answered the question fell. In total, 194 responses yielded losses of $66,930,950 (see figure 16), up from $52,494,290 (for 313 respondents) in 2006. If we look at the average loss per respondent, in 2007 it was $345,005 up from $167,713 in 2006.

[43] http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf



- Spam

Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.[44] E-mail spam, also known as unsolicited bulk email (UBE) or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

Increasingly, e-mail spam today is sent via "zombie networks", networks of virus- or worm-infected personal computers in homes and offices around the globe; many modern worms install a backdoor which allows the spammer access to the computer. Conversely, spam can be used to further distribute malware.

Spam in e-mail started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today comprises some 80 to 85% of all the email in the world, by conservative estimate;[45] some sources go as high as **95%** (i.e Sophos). This level of spam discourages people from using email, greatly decreasing the utility of email, and reduces user's confidence in any online activity. It also threatens the “viability of email for businesses and is reducing the productivity of hundreds of millions of workers around the world.” In terms of productivity and business continuity alone, the losses are enormous. Just the time employees spend each day dealing with spam email can quickly add up to tens of billions.[46]

Sophos conducts analysis of all the spam messages received in the company’s global network of spam traps. Millions of new messages from these honeypots are analyzed automatically every day, and are used to refine and update existing spam rules. [47]

---

44 Wikipedia

45 http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf

46 Cyber Attack: A Risk Management Primer for CEOs and Directors, http://www.acus.org/docs/071212_Cyber_Attack_Report.pdf

47 Security Threat Report 2008, Sophos

In 2007, the chart of the 12 countries relaying the most spam reveals the following:

Dirty Dozen: the top spam-relaying countries in 2007
United States 22.5%
South Korea 6.5%
China (incl HK) 6.0%
Poland 4.9%
Russia 4.7%
Brazil 3.8%
France 3.5%
Germany 3.5%
Turkey 3.1%
Spain 2.7%
Italy 2.7%
India 2.6%
Other 33.5%

Source: Security Threat Report 2008, Sophos

Symantec's latest Internet security treat report shows a different ranking, according to which UK takes one of the forefront positions.[48] Still, the largest share of all spam originated in the United States. Despite the decrease from the previous period, the United States had an eight percent increase in volume of spam messages. The drop in percentage from the United States can be explained by the increase in volume of spam originating in other countries, namely Russia. The prominence of the United States is not surprising, given that it has the highest number of broadband Internet users in the world. The United States was the top country of spam origin for the first half of 2007, as well as the last half of 2006.

Current rank	Previous rank	Country/Region	Current percentage	Previous percentage
1	1	USA	42%	50%
2	3	UK	5%	4%
3	14	Russia	4%	2%
4	2	China	4%	4%
5	7	Poland	3%	3%
6	6	Taiwan	3%	3%
7	4	Japan	3%	4%
8	8	Germany	3%	2%
9	5	South Korea	3%	3%
10	15	Spain	2%	1%

[48] Symantec Global Internet Security Treat Report, Trends for July-December 2007

As security vendors have become more proficient in intercepting stock spam at email gateways, stock-manipulating hackers have turned to more elaborate methods to get their messages in front of internet users. For example, PDF files, JPGs and other image attachments are used to carry the message in the hope that this type of file will be harder to identify as spam.

One of the more bizarre schemes was seen in October 2007 when a pump-and-dump spam campaign used MP3 music files in an attempt to manipulate share prices. Files posing as music from stars such as Elvis Presley, Fergie and Carrie Underwood actually contained a monotone voice encouraging people to buy shares in a little-known company.

The U.S. Computer Emergency Readiness Team (CERT) has been tracking an upswing in targets among the entire online economy, including the financial, aerospace, defense, and computing industries, and reported 80,000 instances in March 2007 alone. It estimates that spam now makes up 94%of all email traffic.

Some estimates claim that the impact of spam is quite significant: costs associated with spam in the United States, United Kingdom, and Canada in 2005 amounted to US$17 billion, US$2.5 billion, and US$1.6 billion, respectively.[49]

A dissertation by Thomas P. Dubendorfer[50] proposes a model for estimating the damage caused by spam in Switzerland: It defines “spam” as unwanted e-mails containing questionable business offers, unsolicited information, phishing attacks or malcode such as, e.g., virus attachments. According to the spam and virus intercept statistics by Message Labs for June 2005, 67.25% of all e-mails scanned for their customers were spam and 1 in 28.16 e-mails scanned contained a virus.

The model investigates the costs caused by productivity loss and by taking preventive measures suffered by enterprises that try to minimise the annoying flood of spam reaching employees.

Productivity loss arises due to an employee having to daily scan through and delete new spam and virus infected e-mails that were delivered to his or her electronic mail inbox. In addition, he or she might need time to install or update a local spam and virus protection on his or her computer. Visiting educational events and reading corporate security related news regarding new e-mail threats is also accounted to productivity loss caused by spam. Assuming an average daily time of 5 minutes wasted on “spam” per employee, the annual economic damage due to productivity loss is estimated at approximately CHF 1.7 billion.

Diverse activities are needed for proper spam prevention: anti-spam system installation and maintenance, user support, reading security news, education of administrators, security awareness events for users, distribution of spam system updates, etc. These activities result in personnel cost and licence fees, which also contribute to the economic damage of spam.

The study calculates the annual personnel cost for fighting spam to be CHF 480 mil, and annual anti-spam licence cost - 24 mil, which result in total annual spam prevention

---

[49] Cyber Attack: A Risk Management Primer for CEOs and Directors, http://www.acus.org/docs/071212_Cyber_Attack_Report.pdf

[50] Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks, A dissertation submitted to the Swiss Federal Institute of Technology, Thomas P. Dubendorfer

cost for enterprises in Switzerland of CHF 504 million. As a result, the total annual economic damage for Switzerland caused by spam is CHF 2.2 billion.

Having in mind this huge economic damage for a small country like Switzerland, there is an apparent need of having a policy for fighting spam effectively.

Estimated Swiss annual economic damage caused by spam

Factor	Symbol	Unit	Spam in CH
Productivity degradation			
Total jobs in CH (100%)			3,590,000.00
IT intense jobs (48.2%)	n_{IT}		1,730,380.00
Annual cost per employee	c_{empl}	CHF/yr	98,075.00
Working time per employee and year		h/yr	1,880.00
Workdays per year	d_{work}	d/yr	230
Daily cost per employee		CHF/d	426.41
Hourly cost per employee	c_h	CHF/h	52.17
Time per day spent on spam e-mails (5 min/d)	$t_{d,spam}$	h	0.08
Daily spam cost per employee $c_{d,spam} = c_h \cdot t_{d,spam}$	$c_{d,spam}$	CHF	4.35
Annual spam cost per employee		CHF	999.88
Total annual productivity loss due to spam $n_{IT} \cdot c_{d,spam} \cdot d_{work}$		CHF	**1.7 bill.**
Spam Prevention Cost			
Statistics about enterprises in CH			
Number of enterprises in CH[a] (100%)			317,739.00
Large enterprises (0.30%)	n_{le}		953.22
Small and medium enterprises SME (11.7%)	n_{sme}		37,175
Micro enterprises (88%)	n_{me}		279,610
Personnel cost (for spam prevention)			
Annual cost per security sysadmin	c_{adm}	CHF/yr	150,000
Annual cost per employee	c_{emp}	CHF/yr	98,075
Large enterprises			
Employment ratio of sysadmin for spam	er_{le}		50%
Annual cost for "spam" sysadmin per large enterprise		CHF/yr	75,000.00
Percentage of large enterprises having e-mail	f_{le}		100%
Total for large enterprises $pers_{le} = n_{le} \cdot c_{adm} \cdot er_{le} \cdot f_{le}$		CHF	71,491,275
SME			
Employment ratio of sysadmin for spam	er_{sme}		3%
Annual cost for "spam" sysadmin per SME		CHF/yr	4,500
Percentage of SMEs having e-mail	f_{sme}		80%
Total for SMEs $pers_{sme} = n_{sme} \cdot c_{adm} \cdot er_{sme} \cdot f_{sme}$		CHF	133,831,667
Micro enterprises			
Employment ratio of dedicated employee for spam (~10 min/d)	er_{me}		2%
Annual cost for "spam" employee per micro enterprise		CHF/yr	1,961.5
Percentage of micro enterprises having e-mail	f_{me}		50%
Total for micro enterprises $pers_{me} = n_{me} \cdot c_{emp} \cdot er_{me} \cdot f_{me}$			274,227,821
Total annual personnel cost $pers_{le} + pers_{sme} + pers_{me}$		CHF	**480 mill.**
Licence cost (for spam prevention)			
Annual licence cost per virus/spam scan solution	lic	CHF/yr	50.00
Large enterprises: annual cost for central spam solution	s_{le}	CHF/yr	10,000
Licence cost for all large enterprises: $n_{sme} \cdot s_{le}$		CHF/yr	9,532,170
SME: number of licences	l_{sme}		5.00
Licence cost for all SME: $n_{sme} \cdot f_{sme} \cdot l_{sme} \cdot lic$		CHF	7,435,093
Micro enterprises: Number of licences		l_{sme}	1.00
Licences for all micro enterprises $n_{sme} \cdot f_{sme} \cdot l_{sme} \cdot lic$		CHF	6,990,258
Total annual licence cost		CHF	**24 mill.**
Total annual cost for spam prevention		CHF	**504 mill.**
Total annual spam damage for Switzerland (ca. $\pm 20\%$)		CHF	**2.2 bill.**

- **Malicious Software (Malware)**

Malicious software, commonly known as "malware", is software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners. Malware can gain remote access to an

information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity.[51]

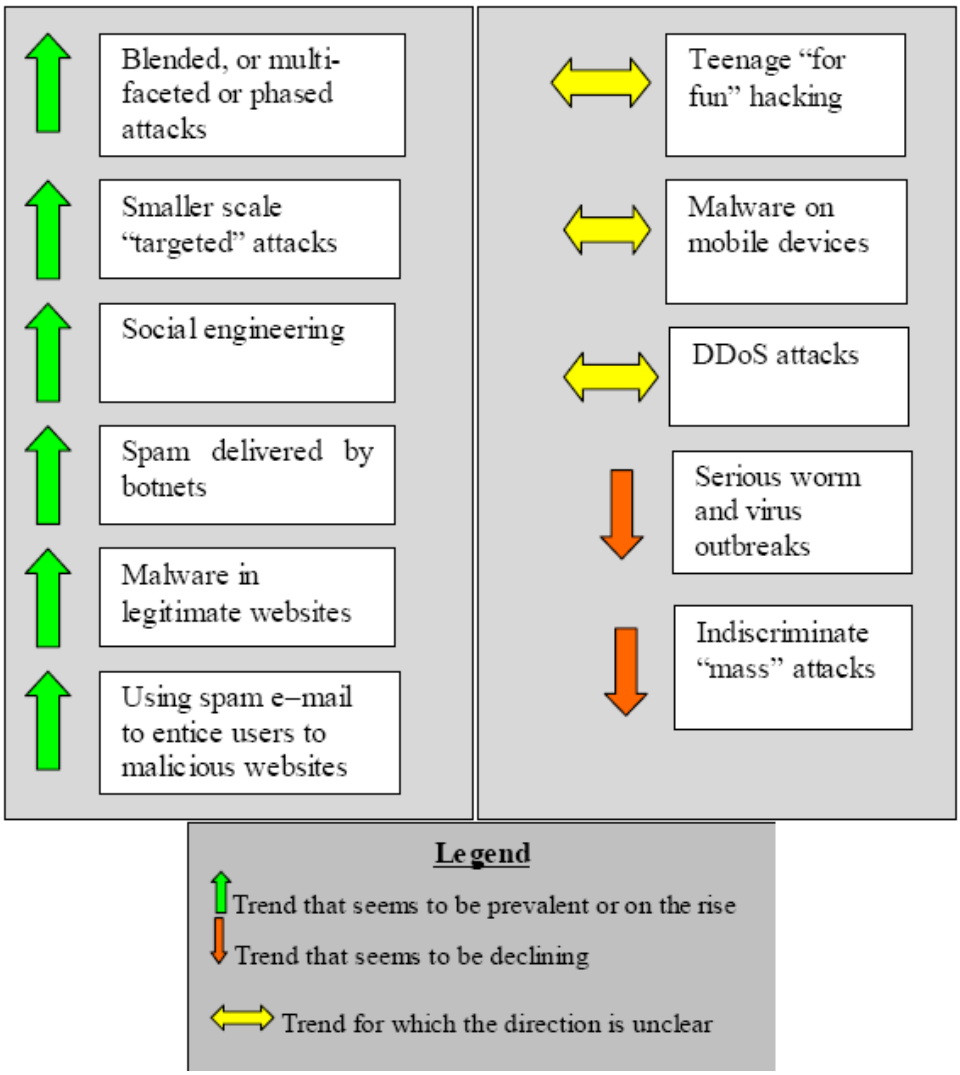
Different types of malware are commonly described as viruses, worms, trojan horses, backdoors, keystroke loggers, rootkits or spyware. These terms correspond to the functionality and behaviour of the malware (*e.g.* a virus is self propagating, a worm is self replicating).

Over the last 20 years, malware has evolved from occasional "exploits" to a global multi-million dollar criminal industry. Malware affects all actors. It is increasingly a shared concern for governments, businesses and individuals. Although its economic and social impacts may be hard to quantify, malware used directly or indirectly can harm critical information infrastructures, result in financial losses, and plays a role in the erosion of trust and confidence in the Internet economy.

The dynamic nature of malware keeps most security experts constantly on the lookout for new types of malware and new vectors for attack. Due to the complex technical nature of malware, it is helpful to examine overall attack trends to better understand how attacks using malware are evolving. The following figure illustrates the types of attack that seem to be on the increase, those that are falling out of favour, and those for which the trend remains unclear or not changed.

[51] OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

General attack trends



Source: OECD, Malicious Software (Malware): A Security Threat to the Internet Economy

Malware is an effective and efficient means for attackers to compromise large numbers of information systems, which cumulatively has the potential to undermine and erode society's ability to trust the integrity and confidentiality of information traversing these systems. The failure to provide adequate protection for the confidentiality and integrity of online transactions may have implications for governments, businesses and consumers.

The nature of malware is such that it is not possible to trust the confidentiality or integrity of data submitted or accessed by any computer host compromised by malware. It is often difficult to readily distinguish a compromised host from one that is not compromised and, as a result, in an environment like the Internet, in which malware has taken hold, connections from infected hosts must be treated as potentially suspect. Therefore, the ability to have trust and confidence in online transactions can be further reduced because traditional mechanisms for building trust and confidence in the

information economy such as authentication, encryption and digital certificates can also be subverted, bypassed or manipulated by malware.

Malware has certain characteristics which make its spread so wide and its impact so big[52]:

- *It is multi-functional and modular*: there are many kinds of malware that can be used together or separately to achieve a malicious actor's goal. New features and additional capabilities are easily added to malware to alter and "improve" its functionality and impact. Malware can insert itself into a system, compromise the system, and then download additional malware from the Internet that provides increased functionality. Malware can be used to control an entire host[53] or network, it can bypass security measures such as firewalls and anti-virus software, and it can use encryption to avoid detection or conceal its means of operation.
- *It is available and user-friendly*: malware is available online at a nominal cost thus making it possible for almost anyone to acquire. There is even a robust underground market for its sale and purchase. Furthermore, malware is user-friendly and provides attackers with a capability to launch sophisticated attacks beyond their skill level.
- *It is persistent and efficient*: malware is increasingly difficult to detect and remove and is effective at defeating built-in information security counter-measures.
- *It can affect a range of devices*: because malware is nothing more than a piece of software, it can affect a range of devices, from personal devices such as personal computers (PCs) or Personal Digital Assistants (PDAs) to servers15 across different types of networks. All these devices, including the routers that allow traffic to move across the Internet to other end points, are potentially vulnerable to malware attacks.
- *It is part of a broader cyber attack system*: malware is being used both as a primary form of cyber attack and to support other forms of malicious activity and cybercrime such as spam and phishing.
- *It is profitable*: malware is no longer just a fun game for script kiddies[54] or a field of study for researchers. Today, it is a serious business and source of revenue for malicious actors and criminals all over the world. Malware, together with other cyber tools and techniques, provides a low cost, reusable method of conducting highly lucrative forms of cybercrime.

There are a number of *challenges to fighting malware*. Protecting against, detecting and responding to malware has become increasingly complex as malware and the underlying criminal activity which it supports are rapidly evolving and taking advantage of the global nature of the Internet. Many organisations and individuals do not have the resources, skills or expertise to prevent and/or respond effectively to malware attacks and the associated secondary crimes which flow from those attacks such as identity theft, fraud and DDoS. In addition, the scope of one organisation s control to combat the problem of malware is limited.

---

52 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy

53 Host refers to a computer at a specific location on a network

54 Script Kiddie refers to an inexperienced malicious actor who uses programs developed by others to attack computer systems, and deface websites. It is generally assumed that script kiddies are kids who lack the ability to write sophisticated hacking programs on their own and that their objective is to try to impress their friends or gain credit in underground cracker communities.

Many security companies report an inability to keep up with the overwhelming amounts of malware despite committing significant resources to analysis. One vendor dedicates 50 engineers to analysing new malware samples and finding ways to block them, but notes that this is almost an impossible task, with about 200 new samples per day and growing.[55] When samples and files are received, security companies undertake a process to determine if the file is indeed malicious. This is done by gathering data from other vendors, conducting automated analysis, or by conducting manual analysis when other methods fail to determine the malicious nature of the code. One vendor estimated that each iteration of this cycle takes about 40 minutes and that they release an average of 10 updates per day. There is always a time lag between when new malware is released by attackers, when it is discovered, when anti-virus vendors develop their signatures, and when those signatures are dated onto users and organisations information systems. Attackers actively seek to exploit this period of heightened vulnerability. In addition, malicious actors exploit the distributed and global nature of the Internet as well as the complications of law and jurisdiction bound by traditional physical boundaries to diminish the risks of being identified and prosecuted. For example, a large portion of data trapped by attackers using keyloggers is transmitted internationally to countries where laws against cybercrime are nascent, non-existent or not easily enforceable.

Sophos currently sees 6,000 new infected webpages each day – one infected page every 14 seconds. Only about 1 in 5 of these sites is a hacker site, i.e. malicious in intent; 83%are hacked sites, or legitimate websites that have been compromised by an unauthorized third-party.[56] Mal/Iframe accounted for over half of all web-based threats in January to December 2007. In June 2007, Mal/Iframe was found to have infected more than 10,000 legitimate Italian websites, including sites belonging to high-profile organizations like city councils, employment services and tourism sites. Most of the affected pages appeared to be hosted by one of the largest ISPs in Italy.

The results of research into which countries contain the most malware-hosting websites reveal the following:

Top ten malware found on the web in 2007
Mal/Iframe 53.3%
Mal/ObfJS 9.8%
Troj/Decdec 6.6%
Troj/Psyme 6.2%
Troj/Fujif 5.8%
JS/EncIFra 3.9%
Troj/Ifradv 2.4%
Mal/Packer 1.2%
Troj/Unif 1.0%
VBS/Redlof 0.8%

[55] Greene, Tim (2007

[56] Security Threat Report 2008, Sophos

Other 9.0%

Source: Security Threat Report 2008, Sophos

The top ten list of the countries containing the most malware-hosting websites puts China, the US and Russia in the lead positions:

Top ten malware hosting countries in 2007
China 51.4%
United States 23.4%
Russia 9.6%
Ukraine 3.0%
Germany 2.3%
Poland 0.9%
United Kingdom 0.7%
France 0.7%
Canada 0.7%
Netherlands 0.7%
Others 6.6%

Source: Security Threat Report 2008, Sophos

Forensic analysis by SophosLabs to determine where malware has been written has revealed some interesting differences in the motives and tactics used by different hacking groups around the globe. For instance, 21 percent of all malware is written in China. This is a smaller proportion than in 2006 when the republic's hackers accounted for 30% of the malicious code seen.

Country % of malware written
China 21.0%
Brazil 12.5%
Russia 9.2%

Source: Security Threat Report 2008, Sophos

Although precise data on online criminal activity and the associated financial losses is difficult to collect, it is generally accepted that malware contributes significantly to these losses.

One association of banks in the United Kingdom estimated the direct losses caused by malware to its member organisations[57] at GBP 12.2 M in 2004, GBP 23.2 M in 2005, and GBP 33.5 M in 2006, an increase of 90% from 2004 and 44% from 2005. Moreover, these direct losses are not fully representative of the actual financial impact as they do not measure diminished customer trust in online transactions, loss in reputation, impact on the brand, and other indirect and opportunity costs that are challenging to quantify. Likewise, they do not include costs such as labour expenses for

[57] Whittaker, Colin (2007)

analysing malware, repairing, and cleansing infected machines, costs associated with the procurement of security tools (such as anti-virus and anti-malware software), or loss of productivity caused by the inability of employees to interact with a system when affected by an attack.

One recent survey of 52 information technology professionals and managers estimated a slight decline in the direct damages associated with malware[58] from EUR 12.2 billion in 2004, to EUR 10 billion in 2005, to EUR 9.3 billion in 2006. This decrease is largely attributed to the suspicion that indirect or secondary losses are actually increasing. Furthermore, the same survey found that most organisations tracked the frequency of malware incidents but not the financial impacts.

Another survey estimated the annual loss to United States businesses at USD 67.2 billion.[59]

Although the malware related costs of security measures are considered proprietary, estimates provided by market players in a recent empirical study[60] ranged from 6-10% of the capital cost of operations. No clear estimates of the effects of malware on operating expenses were available, although the study found that most organisations did experience such effects. There was evidence throughout the empirical research of concern that such effects are important, although no specific indication as to their magnitude is available.

The cost to individual consumers may be even more difficult to measure, however it is likely significant. One example is the United States where consumers paid as much USD 7.8 billion over two years to repair or replace information systems infected with viruses and spyware.[61] While most of this data is not comparable across studies and the surveys are often limited in scope, it does illustrate the magnitude of the financial impact, for both businesses and consumers, resulting from malware.

Viruses, Worms, Trojans

Viruses and worms date back to the early days of computers[62] when most viruses were created for fun and worms were created to perform maintenance on computer systems. Malicious viruses did not surface until the 1980s when the first personal computer (PC) virus, Brain (1986), appeared and propagated when the user "booted up" his/her computer from a floppy disc. Two years later, in 1988, the Morris worm received significant media attention and affected over 6 000 computers. Although other types of malicious software appeared in the mid 80s, the landscape of the late 80s and early 90s predominantly consisted of viruses.

In the mid to late 1990s, the landscape began to change with the growth of the Internet and personal computer use, the rise of networking, and the adoption of electronic mail systems. The so-called "big impact worms" began to reach the public in novel ways. The increased use of e-mail brought high-profile mass-mailer worms such as Melissa

58 Computer Economics (2007)
59 United States Government Accountability Office (2007)
60 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy
61 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy
62 Information based on: OECD, Malicious Software (Malware): A Security Threat to the Internet Economy

(1999), “I Love You” (2000), Anna Kournikova (2001), SoBig (2003) and Mydoom (2004) that made the headlines and entered the public space. These types of worms doubled their number of victims every one-to-two hours, rapidly reaching peak activity within 12-to-18 hours of being released. This marked the parallel rise in organised, sometimes co-ordinated attacks. The explosive growth of online financial transactions resulted in increased security incidents and in the appearance of new types of malicious software and attacks. Today, mass worms and virus outbreaks are becoming ever scarcer while stealthy malware such as trojans and backdoors are on the rise. Many attacks are smaller to stay “below the radar” of the security and law enforcement communities. The goals of the attackers tend to be focused on financial gain. These new trends help explain why malware is now a global multi-million dollar criminal industry.

There are no authoritative figures on the economic cost of computer viruses, worms, Trojan horses, etc. A number of sources make estimates of the cost to business and consumers in respect to individual attacks and yearly costs. These figures are widely cited in the media, however, for the most part the methodologies used to create these figures are not made public. An additional point, made by critics of such data, is that when its producers are security firms or working for security firms, they are not viewed as independent or impartial sources.

Notwithstanding this, the cost of some attacks is most likely significant even if not readily quantifiable.

A survey on the economic impact of cyber-attacks,[63] bases its observations on figures from the two computer security consulting firms most often cited in the media - Computer Economics Inc. and Mi2g. These firms are not primarily research organizations; their data are not published freely, but are available only to subscribers and clients. The figures presented are derived from press accounts and from a limited amount of material made available to CRS on a courtesy basis.

The table below presents Computer Economics (CEI) estimates for the worldwide costs of major virus attacks between 1995 and 2003. Although the data dates back some years ago, it provides a good overview of the scale of the impact of virus attacks.

Annual Financial Impact of Major Virus Attacks, 1995-2003

Year	**Cost ($ billions)**	**Year**	**Cost ($ billions)**
1995	0.5	2000	17.1
1996	1.8	2001	13.2
1997	3.3	2002	11.1
1998	6.1	2003	12.5
1999	12.1		

Source: Computer Economics Inc. Security Issues: Virus Costs Are Rising Again. September 2003,

Mi2g, a British firm, publishes estimates of the costs of worm, virus, and other malicious software attacks, including business interruption, denial of service, data theft

[63] Cashell, Jackson, Jickling, Webel, "The Economic Impact of Cyber-Attacks"

or deletion, loss of sensitive intelligence or intellectual property, loss of reputation, and share price declines.

Worldwide Economic Damage Estimates for All Forms of Digital Attacks, 1996-2004

Year	Cost ($ billions)		Year	Cost ($ billions)	
	Lower	Upper		Lower	Upper
1996	0.8	1.0	2001	33	40
1997	1.7	2.9	2002	110	130
1998	3.8	4.7	2003	185	226
1999	19	23	2004	46	256
2000	25	30			

Source: Mi2g, Frequently Asked Questions: SIPS and EVEDA

The following table presents cost data for specific worm and virus attacks from both CEI and Mi2g. For some attacks, the estimates are very close; for others, they diverge sharply. The differences may reflect either differences in cost estimation models, or the two firms may define the episodes differently. In either case the amounts are very high.

Estimated Costs of Selected Virus and Worm Attacks, 1999-2003 (in billions of dollars)

Attack	Year	Mi2g	CEI
SoBig	2003	30.91	1.10
Slammer	2003	1.05	1.25
Klez	2002	14.89	0.75
BadTrans	2002	0.68	0.40
Bugbear	2002	2.70	0.50
Nimda	2001	0.68	1.50
Code Red	2001	2.62	2.75
Sir Cam	2001	2.27	1.25
Love Bug	2000	8.75	8.75
Melissa	1999	1.11	1.10

Sources: Mi2g figures: Richard Waters, "When Will They Ever Stop Bugging Us?" Financial Times, September 17, 2003, special report, p. 2 (The figures in this table average Mi2g's upper and lower estimates.); CEI figures: Computer Economics Inc. Security Issues: Virus Costs Are Rising Again. September 2003

One research organisation speculates that, at best approximations, a plausible worst-case worm could cause $50 billion or more in direct economic damage to the USA.

Anecdotally, some reputable research has suggested it could be as high as $500 billion[64].

The May 2000 electronic virus "I Love You", which spawned a number of derivative viruses, is estimated to have cost businesses and governments upward of $10 billion dollars.[65]

Numerous organisations and companies make statistics available about their security operations in respect to ICT networks. McAfee, for example, makes statistics available in relation to its operations on a global basis. These include a map of the world showing the extent of virus activity by country. The McAfee data, on the most prevalent viruses, are also broken out by region.[66]

The SANS Institute, estimated that clean up cost of two worms exceeded USD 1 billion each in 2003.[67] For the same year Trend Micro, a leading security company, estimated the global cost of viruses to be USD 55 billion compared to USD 30 billion in 2002. Prevx, a software security company, put the total cost of the ten most damaging worms at USD 17.2 billion for the year 2004. Some other sources put the global costs even higher than those mentioned but the results of these figures, and those cited above, are not verifiable.[68]

Respondents to the CSI/FBI survey, in the United States, and the AusCERT survey, in Australia, report the following losses stemming from viruses, worms and Trojans in 2004: USD 55 million (United States) and USD 5.6 million (Australia).

In Consumer Reports 2005 "State of the Net", the authors stated the overall incidence was of Viruses was rising with more targeting of confidential information with 1 in 4 respondents experiencing a major, often costly problem. Consumer Reports further stated that the average cost per incident to consumers was USD 312, producing a national total of USD 5.5 billion in losses in the United States.

In the UK, viruses and malicious software continue to be the most common cause of security incidents. In 2005, over a third of firms suffered a virus or disruptive software incident, although this figure is a reduction from 50% in 2004. In 2007, it is clear that malware causes much less direct damage than in the past. Only 14% of UK companies had a malware infection in 2007. Even among very large businesses, less than half had an infection. However, despite the lower levels of infection, it would be a mistake, however, to assume that the malware threat is extinguished. For two-thirds of companies that had a virus infection, it was their worst security incident of the year. Malware infections were particularly damaging in the telecommunications sector.[69]

Spyware

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. While the term spyware suggests software that secretly

64 DTi, Changing nature of information security – a UK perspective on US experiences

65 *Investor's Business Daily*, May 17, 2000, Sec. A, p. 9.

66 The map is available at: http://us.mcafee.com/virusInfo/default.asp?cid=10371

67 The SANS Institute, "The Top 20 Internet Security Vulnerabilities and How to Eliminate Them", 2003, http://www.sans.org/top20/cdipresentation.pdf

68 OECD, Scoping Study for the Measurement of the Trust in the Online Environment

69 2008 Information security Breaches Survey, BERR

monitors the user's behaviour, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs.[70]

McAfee detected fewer than 2 million "adware or spyware" products in August 2003. By March 2004, the total number had increased to just more than 14 million.[71]

Symantec's bi-annual report provides analysis and discussion of trends in Internet attacks, including malicious code created to expose confidential information. The report for the period July to December 2007 documented a steep increase in this phenomenon.

In 2005, Microsoft released a test version of a new anti-spyware program and made it freely available to Windows users. The software has the capability to let users remit information anonymously to Microsoft and, by February 2005, the company was receiving half a million reports per day.101

The cost of spyware Some security experts warn that spyware is already causing some financial institutions to scale back the range of services they offer to users and to damage trust in respect to electronic commerce.102 At the same time little data are available that would inform an estimate of the cost of spyware, as a proportion of overall identity crime, to business and consumers. Some indirect indicators are available. In 2004, McAfee reported that spyware became a larger technical support problem than viruses in terms of customer calls.

The experience of other companies appears to confirm that together spyware and viruses generate the largest losses and most concern to users.

According to Dell, the world's largest supplier of personal computers, "…a record number of customers contacting Dell with computer performance issues caused by spyware and viruses shows how pervasive the problem is among home technology users. Up to 20% of the calls received by Dell's consumer desktop technical support team are for spyware and virus-related issues, far surpassing any other performance issue."[72] One panellist at the FTC Workshop reported that the average call to an ISP helpdesk lasts 6 minutes whereas the average for a call involving spyware is 25 minutes. At the same time, Microsoft says that over one-third of the users reporting crashes in their applications are actually dealing with spyware problems. Occurences such as these generate costs for business and consumers as well as impacting on the confidence users have in suppliers of equipment and services to which they may attribute problems generated by spyware. [73]

In March 2005, it was reported that Police in the United Kingdom had thwarted an attempt to use spyware against a Bank, in an attempt to illegally transfer USD 423

---

70 Wikipedia

71 http://news.cnet.com/Few-solutions-pop-up-at-FTC-adware-workshop/2100-1028_3-5195222.html

72 Dell, "Dell Launches Campaign to Build Awareness of PC Security Issues", Press Release, Round Rock, Texas, 20 July 2004

73 OECD, Scoping Study for the Measurement of the Trust in the Online Environment

million.[74] In this instance the perpetrators used "keylogging" software that enabled them to track internal entries on computer keyboards.

Criminals are successfully earning revenue from spyware, which appears to be reflected in the fact that they are also making unsolicited offers to software developers. In February 2005, the Internet Storm Center reported offers that would return USD 0.25 per installation of a program that included three pieces of embedded spyware.[75]

As the market for Internet advertising has increased, the economics of the grey area between spyware and adware appears to have increased in attractiveness. Webroot, an anti-spyware company, has put the average return from a "spyware or adware" installation at USD 2.40 per year.[76] This revenue is gained from charging fees from pop-up advertising, redirecting users to Web pages and so forth. Accordingly to Webroot's estimates, the three programmes in this category with the largest installed base worldwide may generate close to USD 0.5 billion per year.

Economists have also begun to explore the returns on investment (ROI) in security against various forms of Internet phenomenon from spam to spyware, from the perspective of attackers (ROA). While this work is producing econometric models, which can be employed for such analysis, the availability of data tends to be a limitation.

In Consumer Reports 2005 "State of the Net", the authors stated the overall incidence of Spyware was undergoing "explosive growth" with 1 in 6 respondents experiencing a major, often costly problem. Consumer Reports further stated that the average cost per incidence to consumers was USD 250, producing a national total of USD 3.5 billion in losses in the United States.

Phishing and keystroke logging (keylogging)

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking, or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts. A phishing Web site is a site that is designed to mimic the legitimate Web site of the organization whose brand is being spoofed. In many cases, it is set up by the attacker to capture a victim's authentication information or other personal identification information, which can then be used in identity theft or other fraudulent activity. [77]

The majority of brands used in phishing attacks in the last six months of 2007 were in the financial services sector, accounting for 80%, virtually unchanged from the 79% reported in the previous period. The financial services sector also accounted for the highest volume of phishing Web sites during this period, at 66 %. Since most phishing activity pursues financial gain, successful attacks using brands in this sector are most likely to yield profitable data, such as bank account credentials, making this sector an obvious focus for attacks.

---

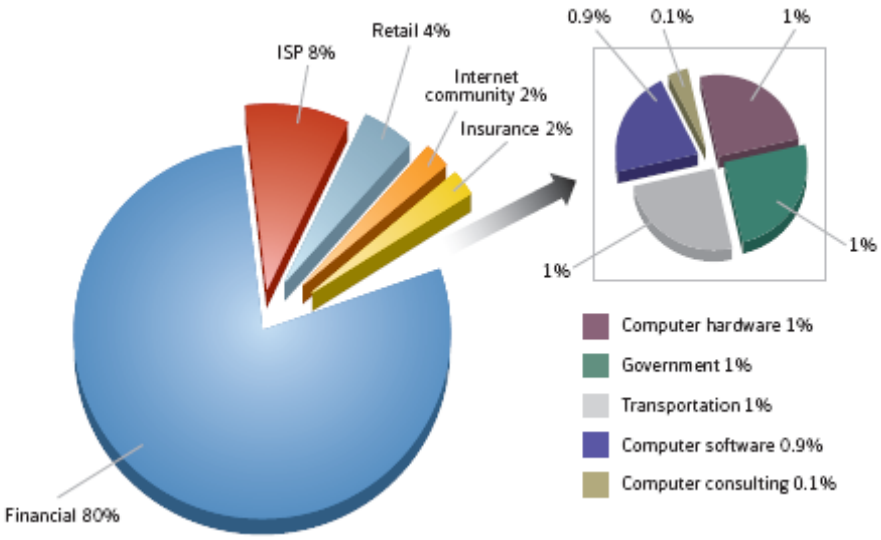
74 BBC, "UK police foil massive bank theft", 17 March 2005, http://news.bbc.co.uk/2/hi/uk_news/4356661.stm

75 ISC, Handlers Diary, 27 February 2005. http://isc.sans.org/index.php?off=worldmap

76 OECD, Scoping Study for the Measurement of the Trust in the Online Environment

77 Symantec Global Internet Security Threat Report

Unique brands phished by sector



- Source: Symantec Corporation

In the second half of 2007, 66% of all phishing attacks detected by Symantec were associated with Web sites located in the United States. For phishing attacks with Web sites hosted in the United States, all of the top 10 targets are also headquartered there. China hosted the second most phishing Web sites, with 14% of the total. The top target phished by Web sites hosted in China was the same social networking site most commonly phished by Web sites in the United States, accounting for 96% of phishing Web sites hosted in China.

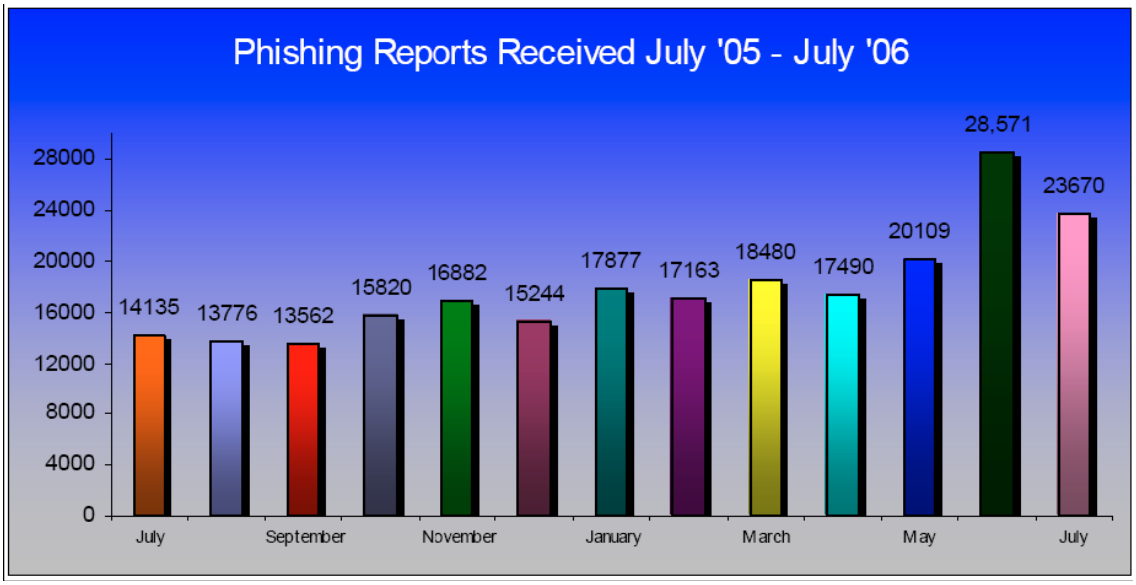
Top countries hosting phishing Web sites and top targets phished

Rank	Country	Percentage	Top Target Phished
1	United States	66%	Social networking site
2	China	14%	Social networking site
3	Romania	5%	Social networking site
4	Guam	5%	Social networking site
5	France	1%	Online auction site
6	Germany	1%	Online payment system
7	Italy	1%	Online auction site
8	Canada	1%	Online portal
9	Sweden	1%	Telecommunications provider
10	Netherlands	1%	Social networking site

Source: Symantec Corporation

The Antiphishing Working Group (APWG), which collects and publishes very useful information and best practice documents, reports the following situation about phishing[78]:

[78] http://www.antiphishing.org (High Tech Crimes Within the EU: Old Crimes New Tools, New Crimes New Tools, 2007)



The cost of phishing. Estimates for the cost of phishing vary widely. At one end of the scale some individual financial institutions, while not willing to reveal their own financial losses, say the sums are relatively modest. In March 2005, APACS, the United Kingdom's Association for Payment Clearing Services, put the cost of online baking fraud (primarily made up of phishing), to its members in the United Kingdom, at £23 m for 2005. [79]

A study conducted by the Ponemon Institute in 2004[80], revealed that 76% of consumers in the United States were experiencing an increase in spoofing and phishing incidents and that 35% receive fake e-mails at least once a week. The report estimated the total monetary loss to victims of these incidents to be approximately USD 500 million in the United States.

Gartner has also attempted to quantify the cost of phishing in the United States. Gartner's results suggest a larger scale of problem. In a study published in May 2004, Gartner estimated direct losses from identity theft fraud against phishing attack victims, in the United States, had cost banks and credit card issuers about USD 1.2 billion during 2003. For 2005, Gartner estimates the figure at over USD12 billion.

Other studies with a broader geographical coverage are also at odds over losses due to phishing. According to the TowerGroup the global losses from phishing via e-mail were in the vicinity of USD 137 million in 2004. The TowerGroup said the actual number of phishing attacks totaled more than 31 000 globally in 2004 and that they expect this to rise to over 86 000 in 2005.

This raises the question of why estimates of the direct losses attributed to victims of phishing vary so greatly. In part this may be because financial institutions, while taking the threat seriously, are reluctant to publicly reveal their losses. In addition some firms may simply not know the scale of losses if they go unreported by their customers. Taken together these factors may mean that it would be very difficult for industry to determine a definitive figure for the direct financial losses attributable to phishing.

[79] "Changing nature of information security – a UK perspective on US experiences"

[80] "U.S. Consumer Loss of phishing Fraud to Reach $500 Millon", 29 September 2004, http://www.truste.org/about/press_release/09_29_04.php

The APWG report that by hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients of spoofed e-mails to respond. In the United Kingdom, APACS has commissioned research which showed that 4% of Internet banking users would respond to an e-mail, supposedly from their bank, asking them to click on a link and re-enter their security details. Based on survey data, Gartner estimates that about 19% of those attacked, or nearly 11 million adult Internet users in the United States, have clicked on the link in a phishing attack e-mail. Gartner further report that 3% of those attacked, or an estimated 1.78 million adults in the United States, reported giving phishers their financial or personal information in 2003.[81]

The Ponemon Institute study, based on a national sample of 1 335 Internet users across the United States, recorded that seven out of ten respondents had unintentionally visited a spoofed Web site. The study reported that more than 15% of spoofed respondents admitted to being "phished" in that they had provided private information. In total, the study found, a little more than 2% of all respondents believed that they experienced a direct monetary loss resulting from the phishing attack.

In Consumer Reports 2005 "State of the Net", the authors stated the overall incidence was of Phishing was rare but rapidly increasing with 1 in 200 respondents losing money from their account. Consumer Reports further stated that the average cost per incidence was USD 395 producing a national total of USD 147 million in losses for the United States. [82]

Malware on mobile devices

There is some debate around the current seriousness of threats to mobile devices such as cell phones, PDAs, and smartphones.[83] For example, some factors seem to indicate that threats to mobile devices are still limited.[84] These factors include the following:

- some of the current forms of mobile attacks can only be launched within the 10 metres personal area network (PAN)[85] range - which limits the scope of the danger compared to traditional malware threats which have a global reach;

- mobile devices are restricted by bandwidth because there is a limited amount of spectrum allocated for their use;

- the very small user interface is still an impediment to conducting Internet banking and other value transactions – until mobile devices become a popular means to conduct such transactions there are fewer incentives for attackers to develop malware for the mobile telephone platform;

- the cost associated with using general packet radio service (GPRS) to connect to Internet Protocol (IP) data networks may also make the mobile device less popular

81 OECD, Scoping Study for the Measurement of the Trust in the Online Environment

82 OECD, Measurement of Trust In The Online Environment

83 A Smartphone is a cellular phone coupled with personal computer like functionality

84 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy

85 A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves, or for connecting to a higher level network and the Internet.

compared to Internet-connected PC which use technologies such as asymmetric digital subscriber line (ADSL), cable or broadband wireless.

However, there is also recognition that such threats, while emerging, are quite real. Some data shows that although still relatively small in comparison to the amount of PC malware, mobile malware, which first appeared in 2004, increased from only a few instances to over 300 in total in a two-year period.[86] Further, concerns about security increase as mobile devices become more prevalent and are used to access more critical or "valuable" services. For example, the use of smartphones is on the rise with projections as high as 350 million in use by 2009. [87] In 2006, Apple announced that a number of video iPods had been shipped to customers with the RavMonE virus.[88] Many experts are concerned that mobile malware will soon become far more dangerous to the mobile devices themselves, the wireless networks over which those devices communicate and the corporate networks, servers and/or personal computers with which those devices exchange information. Undetected malware on a smartphone could get transferred to a corporate network and used to perform further malicious functions.[89]

In its 2004 Global Security Index Report, IBM identified cellular mobile phones and PDAs as a new frontier for viruses, spam and other potential security threats.[90] In 2004, the first “worm” targeted at mobile telephones appeared. The so-called Cabir worm spreads via Bluetooth.

By February 2005, according to F-Secure a Finnish security company, the Cabir virus had spread to 14 countries.[91] In the same month a number of high profile invasions of privacy occurred in respect to cellular mobile telephones. In March 2005, F-Secure announced they had found the first virus capable of spreading via multimedia messaging services, which contain photos, sound or video clips, over mobile phones.

According to Sophos, there are currently approximately 200 malware threats for mobile phones, compared to over 300,000 for Windows. Thus, the risk of being infected on a mobile phone is tiny in comparison. Nevertheless, the mobile malware threat has been growing steadily over the last few years and more businesses are now looking to secure confidential data against potential attacks at all endpoints. In a Sophos web poll, in November 2006, 81% of business IT administrators expressed concern that malware and spyware targeting mobile devices will become a significant threat in the future. However, 64% also said they currently have no solution in place to secure company smartphones and PDAs.[92]

Botnets

A “botnet” is a group of malware infected computers also called “zombies” or “bots” that can be used remotely to carry out attacks against other computer systems. BOTs can turn such computers into vehicles to attack and disable other computer systems and network components, e.g., routers, including those of critical (information)

---

86 Hypponen, Mikko (2006)

87 Hypponen, Mikko (2006)

88 http://www.apple.com/support/windowsvirus/

89 iGillottResearch Inc (2006)

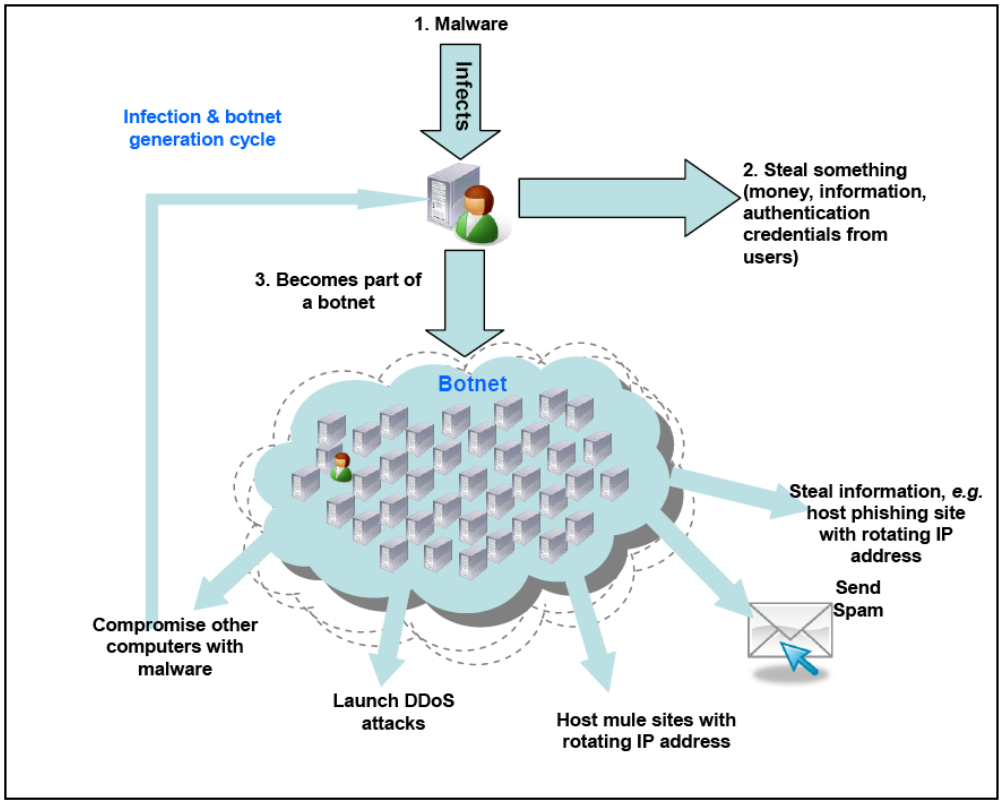
90 “IBM report: Surge in viruses and worms targeting mobile devices, satellite communications anticipated in 2005”, 9 February 2005, http://www-1.ibm.com/services/us/index.wss/rs/imc/a1008866.

91 http://www.f-secure.com/weblog/

92 Security Threat Report 2008

infrastructure providers as well as other important international organizations. The risk grows commensurately as more high power PCs are connected at ever higher speeds of connectivity.

Bots are generally created by finding vulnerabilities in computer systems, exploiting these vulnerabilities with malware, and inserting malware into those systems, inter alia. Botnets are maintained by malicious actors commonly referred to as "bot herders" or "bot masters" that can control the botnet remotely. The bots are then programmed and instructed by the bot herder to perform a variety of cyber attacks, including attacks involving the further distribution and installation of malware on other information systems. Malware, when used in conjunction with botnets, allows attackers to create a self-sustaining renewable supply of Internet-connected computing resources to facilitate their crimes:



There is a cyclical relationship: malware is used to create botnets, and botnets are used to further distribute spam and malware. When malware infects an information system, two things can happen: something can be stolen (e.g, information, money, authentication credentials etc.) and the infected information system can become part of a botnet. When an infected information system becomes part of a botnet it is then used to scan for vulnerabilities in other information systems connected to the Internet, thus creating a cycle that rapidly infects vulnerable information systems.[93]

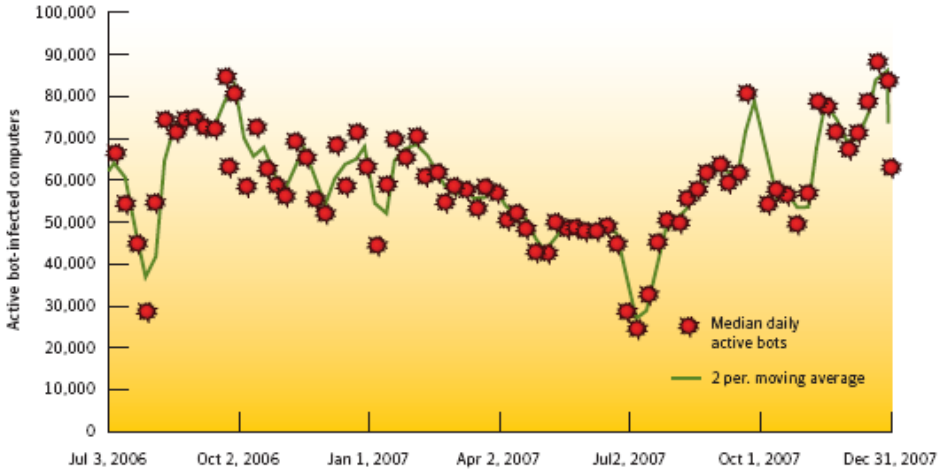
The same OECD survey classifies the different uses of botnets. According to it botnets are mostly used for the following purposes:

[93] OECD, Malicious Software (Malware): A Security Threat to the Internet Economy

- Locate and infect other information systems with bot programmes (and other malware). This functionality in particular allows attackers to maintain and build their supply of new bots to enable them to undertake the functions below, *inter alia*.
- Conduct distributed denial of service attacks (DDoS).
- As a service that can be bought, sold or rented out.
- Rotate IP addresses under one or more domain names for the purpose of increasing the longevity of fraudulent web sites, in which for example host phishing and/or malware sites.
- Send spam which in turn can distribute more malware.
- Steal sensitive information from each compromised computer that belongs to the botnet.
- Hosting the malicious phishing site itself, often in conjunction with other members of the botnet to provide redundancy.
- Many botnet clients allow the attacker to run any additional code of their choosing, making the botnet client very flexible to adding new attacks.

The prevalence of botnets has been increasing. Although estimates of the number of botnets can vary widely, most experts agree it is a large amount.
For example, Symantec's latest Security threat report observed an average of 61,940 active bot-infected computers per day in the second half of 2007, an increase of 17% from the previous period. (An active bot-infected computer is one that carries out an average of at least one attack per day. This does not have to be continuous; rather, a single computer can be active on a number of different days). Symantec gather the data on bot-infected computers from their monitoring of 20 000 sensors located in networks in over 180 countries. Attacks from infected computers are recorded and matched against other databases such as for malicious codes and those enabling the assessment of originating addresses.

Active bot-infected computers by day



Source: Symantec Corporation

Symantec also observed 5,060,187 distinct bot-infected computers during this period, a one percent increase from the first six months of 2007. A distinct bot-infected computer is a distinct computer that was active at least once during the period. The average lifespan of a bot-infected computer during the last six months of 2007 was four days.

The United States had the most bot-infected computers, accounting for 31% of the worldwide total. Madrid was the city with the most bot-infected computers, accounting for three percent of the worldwide total. In the last six months of 2007, Symantec identified 4,091 bot command-and-control servers. This is an 11% decrease from the previous reporting period, when 4,622 bot command-and-control servers were identified. Of these, 45% were located in the United States, more than any other country. Symantec has suggested that the large share attributed to the countries at the top of the ranking may be due to rapid broadband growth in those countries.

Malicious activity by country

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Bot Rank
1	1	United States	31%	30%	1
2	2	China	7%	10%	3
3	3	Germany	7%	7%	2
4	4	United Kingdom	4%	4%	9
5	7	Spain	4%	3%	4
6	5	France	4%	4%	8
7	6	Canada	3%	4%	13
8	8	Italy	3%	3%	5
9	12	Brazil	3%	2%	6
10	9	South Korea	2%	3%	15

Source: Symantec Corporation

While botnets vary in size, they typically number tens of thousands of compromised computers. There have been exceptions including a group of attackers in The Netherlands who reportedly controlled 1.5 million bots.[94]

In 2006, the Chinese National Computer Network Emergency Response Technical Team Coordination Centre (CNCERT/CC) reported that 12 million IP addresses in China were controlled by botnets.[95] They also found more than 500 botnets and more than 16 000 botnet command and control servers outside China.

There seems to be a correlation between the increased threat of botnets can and the increased use of broadband connections to access the Internet. Further efforts are needed from users, as we ell as providers, to protect their security and privacy in the online environment. At the end of 2005, there were around 265 million active subscribers to fixed Internet connections in OECD countries. Of these, 60% were using broadband access, and broadband subscriptions have increased by more than 60% a year over the last five years. By mid-2006, there were more than 178 million broadband subscribers in the OECD area. European countries have continued to advance, with

[94] Govcert.nl (2006)
[95] Dr. Du, Yuejun (2007)

Denmark, the Netherlands and Iceland overtaking Korea and Canada in terms of broadband penetration rates over the past year. The broadband transition to faster upload bandwidth via fibre could make the botnet problem much more severe. The potency of one infected computer on a fibre connection could be equivalent to 31 infected computers on DSL and 44 computers on cable networks. One infected computer on a fibre connection with 100 Mbit/s of upload capacity could theoretically cause as much damage as 390 infected computers with upload speeds of 256 kbit/s. The average advertised upload speeds for broadband in the OECD in October 2006 was 1 Mbit/s for DSL, 0.7 Mbit/s for cable and 31 Mbit/s for FTTx. This will be one of the key areas of concern for policy makers dealing with telecommunication networks and security in the near future. [96]

The cost of botnets

With so many PCs now infected, competition to supply botnets has become intense and the cost of buying and leasing them has tumbled. Botnets have become a contracted commodity. Malicious actors can hire or buy a bot master to carry out an attack. Around 5% of all global machines may be zombies – and the cost of renting a platform for spamming is now around $0.37 per zombie per week[97].

Some security professionals report that botnets can be hired over the Internet via electronic mail, Web pages and IRC (Internet relay chat) networks.[98] One report averaged the weekly rental rate for a botnet at USD 50 – 60 per 1 000 – 2 000 bots or around 33 cents per compromised computer.[99] This is extraordinarily cheap compared to the cost of the computer to the legitimate owner in terms of hardware, software and bandwidth.

Another offer indicated a botnet with 5 000 machines could be hired for USD 300. A number of security professionals quoted in various media reports indicate that botnets with 1 000 machines are available for around USD 100 per hour. The demands of extortionists can vary depending on the potential losses hackers feel they can inflict on a business by bringing down their Web site. In one case an attacker told an agent of the National Hi-Tech Crime Unit, posing as another hacker, that he demanded USD 5 000 to USD 10 000 to cease attacks depending on the size of the site.

According to another estimation there are at least 1000 difference Botnet C&C servers running constantly. An average C&C server controls 20.000 compromised computers (ranging from 10-300.000). Estimations indicate ca 53.000, new, active bots/day. A spam bot can send up to 3 spam emails/s (ca 259.000 emails/day).[100]

Illicit revenues produced by the utilization of BOTNETS are huge. Recently, the American federal authorities13 arrested a young hacker of 20 years of age who was able to manage 400,000 compromised computers, spreading a Trojan horse called ‘rxbot’. It is believed he had already gained $60,000 and a BMW car through his illegal activities.[101]

---

96 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy

97 Personal Internet Security, UK House of lords report, http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

98 OECD, Scoping Study for the Measurement of the Trust in the Online Environment

99 MessageLabs (2006)

100 The European files, April 2008; Article: NIS Security: A constant challenge for ENISA

101 Security Threat Report 2008, Symantec

Amongst other targets, the computer systems of the Weapons Division of the US Naval Air Warfare Centre and the US Department of Defence's Information Systems Agency have been attacked. Critical infrastructure systems can also be targeted by BOTS, as well as the financial sector which is heavily affected by this issue.

The examples given above are real proof of how this phenomenon is evolving and the myriad of possibilities that it can offer, which can also include extortion perpetrated by the hackers threatening the target who can potentially be under attack.

DoS/DDoS attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely, by overwhelming it with an unusually large volume of traffic.[102] Popular targets include companies that conduct business online and risk losing significant revenue for every minute their website or network is unavailable, and governments who rely on websites to provide essential services to their citizens. These attacks are usually used for sabotage (for example, to hurt a competitor or an organisation against whom the attacker holds a grudge or grievance), extortion, or for politically and ideologically motivated purposes.

DDoS is considered the number one concern for large IP network operators according to the Worldwide Infrastructure Security Report[103]. Forty-six percent of the survey participants said DDoS is the most significant operational security issue they face today. Bots and botnets come second, with 31% of the respondents listing them as their primary operational security concern:

46% – DDoS

31% – Bots and Botnets

7% – Worms

6% – Compromised Infrastructure

6% – DNS

4% – BGP Route Hijacking

The effects of a DDoS attack extend far beyond direct financial losses at the time of the attack. Already at the beginning of 2000 Avi Goldfarb at the University of Toronto in Canada examined the indirect effect of a DoS attack by monitoring 2700 volunteers with dial-up connections for three months. During that period, a hacker called Mafiaboy orchestrated a three-hour DoS attack against Yahoo. Two weeks later, many users who had been forced to switch sites during the DoS attack were still visiting Yahoo's rivals MSN, AltaVista and Excite, and seemed to have a preference for one of the alternatives. Three months after the attack, Yahoo users were still more likely to be visiting rival sites, but by then they had no preference for a single rival, Goldfarb told the WEIS conference. They were simply punishing Yahoo for what they perceived to be bad

[102] Wikipedia

[103] Worldwide Infrastructure Security Report, Arbor Networks

service during the DoS attack, he says. Overall, Yahoo lost 6 million unique visitors and $250,000 in revenue.[104]

In 2004 a number of cases of extortion were reported whereby the owners of e-commerce Web sites were threatened with denial of service attacks.[105] Online gambling Web sites have been one of the primary targets but also firms engaging in Web-based financial transactions. In one case, National Hi-Tech Crime Unit, hackers targeted the Web site of an online bookmaker in the United Kingdom with a denial of service attack. The hackers told the bookmakers that they would cease if the bookmakers transferred USD 40 000 to an account in a Latvian bank. The bookmaking firm agreed and transferred money several times, but when the attacks continued they contacted the National Hi-Tech Crime Unit. According to the case brought against the alleged culprits, in Russia, the total losses suffered by the victims of this particular gang were put at USD 3 million. This was an estimate of lost business and payments made to the alleged extortionists. Losses would however be difficult to quantify in many cases. Recent academic research suggests there is a lasting negative impact on Web sites that become unavailable due to denial of service attacks. The research suggests sites with a low switching cost are worse hit by such attacks.[106]

In 2004 well-known companies such as Akamai and Doubleclick were also subject to denial of service attacks.[107] In one well-reported case an individual, currently on the FBI's most wanted list, is alleged to have hired hackers, using botnets of between 5 000 to 10 000 machines, to launch denial of service attacks against his company's competitors. In 2005 it was reported that botnets were being used to compromise Google's "Adwords" advertising campaign by inflating the number of times an advertisement is displayed. Some businesses report extortion demands of between USD 30 000 to USD 50 000 in the face of denial of service attacks.

DDoS attacks have been launched against governments for various purposes including political or ideological ones. For example, Swedish government websites were attacked in the summer of 2006 as a protest against the country's anti-piracy measures. More recent events in Estonia have raised an interesting discussion on what a cyber attack of this nature means for countries.

- Security/data breaches

Probably the most in-depth study of the costs associated with security breach notifications has been that conducted by the Ponemon Institute.[108] It examines the costs incurred by 35 organizations after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. Breaches included in the survey ranged from less than 4,000 records to more than 125,000 records from 15 different industry sectors.

---

104 http://www.eurekalert.org/pub_releases/2005-06/ns-ttc062205.php

105 Netcraft, "E-commerce Firm 2Checkout Reports DDoS Extortion Attack", 17 April 2004, http://news.netcraft.com/archives/2004/04/17/ecommerce_firm_2checkout_reports_ddos_extortion_attack.html

106 OECD, Scoping Study for the Measurement of the Trust in the Online Environmen

107 Netcraft, "Akamai Attack Highlights Threat From Bot Networks", 16 June 2004, http://news.netcraft.com/archives/2004/06/16/akamai_attack_highlights_threat_from_bot_networks.html and "DDoS Attack on DoubleClick Slows Many Sites", 28 July 2004, http://news.netcraft.com/archives/2004/07/28/ddos_attack_on_doubleclick_slows_many_sites.html

108 http://www.ponemon.org/press/PR_Ponemon_2007-COB_071126_F.pdf

Among the study's key findings[109] are:

• **Total costs increase:** The total averages costs of a data breach grew to $197 per record compromised, an increase of 8% since 2006 and 43% compared to 2005. The average total cost per reporting company was more than $6.3 million per breach and ranged from $225,000 to almost $35 million.

• **Cost of lost business accelerates:** The cost of lost business continued to increase at more than 30%, averaging $4.1 million or $128 per record compromised. Lost business now accounts for 65% of data breach costs compared to 54% in the 2006 study.

• **Third-party data breaches increase, and cost more:** Breaches by third-party organizations such as outsourcers, contractors, consultants, and business partners were reported by 40% of respondents, up from 29% in 2006 and 21% in 2005. Breaches by third parties were also more costly than breaches by the enterprise itself, averaging $231 compared to $171 per record.

• **Other data breach costs decrease, as response to breaches matures:** Other costs associated with a data breach decreased 15% from 2006. The costs include investigations, notification of impacted individuals, and services such as offering free credit monitoring. This decrease appears to indicate that organizations are learning from past breach responses and are being more measured in their response by offering fewer free services, for example.

• **Encryption and data loss prevention use increase following a breach:** Encryption and data loss prevention (DLP) solutions were the top two technology responses following a data breach. This finding indicates that organizations increasingly understand the benefits of enterprise data protection in securing data wherever it is stored or used. Additional study findings:

• **Increased customer churn rates help drive lost business costs higher:** In 2007, the average resulting abnormal customer churn rate was 2.67%, an increase from 2.01% in 2006. Greater customer turnover leads to lower revenues and a higher cost of new customer acquisition resulting from increased marketing to recover lost customer business.

• **Legal defense, public relations costs increase:** Indicating continued growing dissatisfaction and action over a data breach, the costs organizations expended for legal defense and public relations grew to 8% and 3% of total breach costs, respectively.

• **Lost and stolen laptops and mobile devices continue as most frequent cause of a data breach:** Almost half (49%) of data breaches in the 2007 sample were due to lost or stolen laptops or other devices such as USB flash drives.

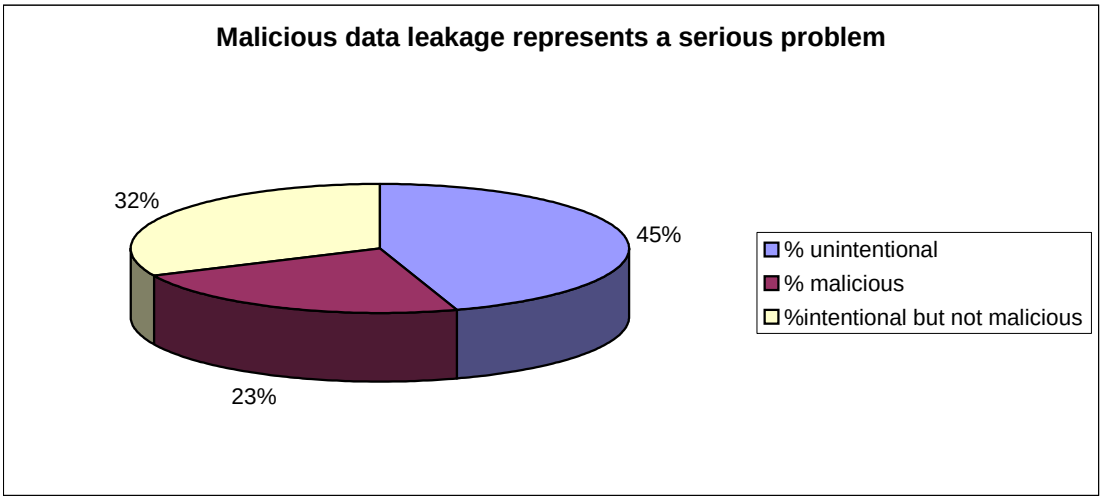
• **Financial services firms impacted most:** The cost of a data breach for financial services organizations was $239 per compromised record, or more than 21% higher than the average, demonstrating that organizations with high expectations of trust and privacy have more to lose from a data breach.

• **Incident response roles and responsibilities**: The group most frequently involved in the response to a data breach was the legal department (79% of organizations); however, IT shared responsibility for breach response in 51% of organizations.

[109] 2007 Annual Study: US Cost of a data breach

Acquisti et al, analyzed the effect of data breaches on the stock market prices of firms that had publicly announced data breaches. They found that data breaches have a transient, but statistically significant, negative impact on the breaching company's stock price. Furthermore, stock market participants appear to react more negatively to announcements by retail firms, intentional or malicious hacking or attempts to access data, and very large data breaches.

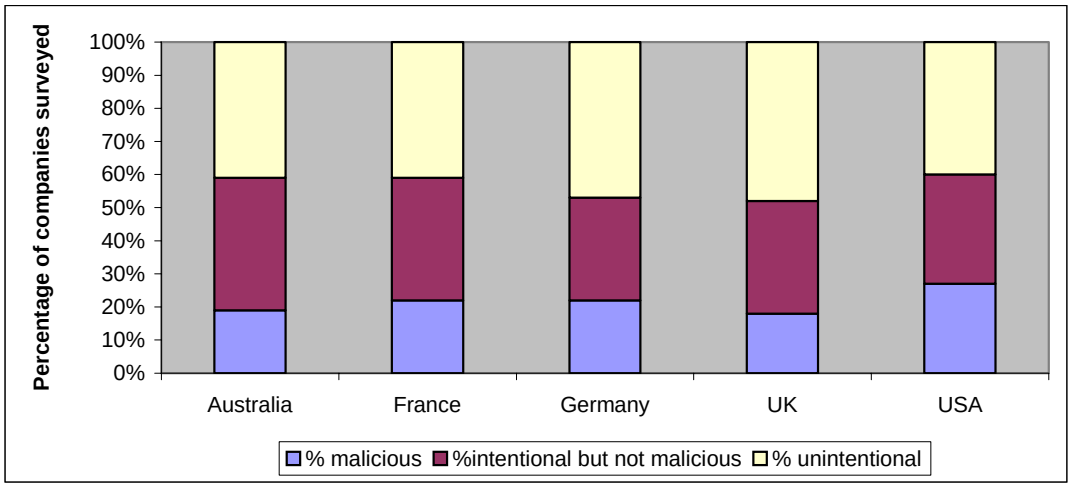
A study by McAfee[110] sees the problem of data loss as one that is growing exponentially. Nearly 150 million records containing sensitive personal information have been involved in data breaches only in the US. Since 2004, there has been a 1700% increase in data loss incidents. In December 2006, the number of data loss incidents hit 100 million; by spring of 2007, the number grew to 150 million.



Source: Datagate: the next inevitable corporate disaster

Geographical analysis shows that the perception of intentional data leakage is higher in the United States and France (close to 30%). This could be a result of a more mobile workforce that travels frequently or works at home and routinely uses remote access, PDAs, laptops and cell phones.

US and French enterprises experience more intentional leakage



[110] Datagate: the next inevitable corporate disaster, McAfee

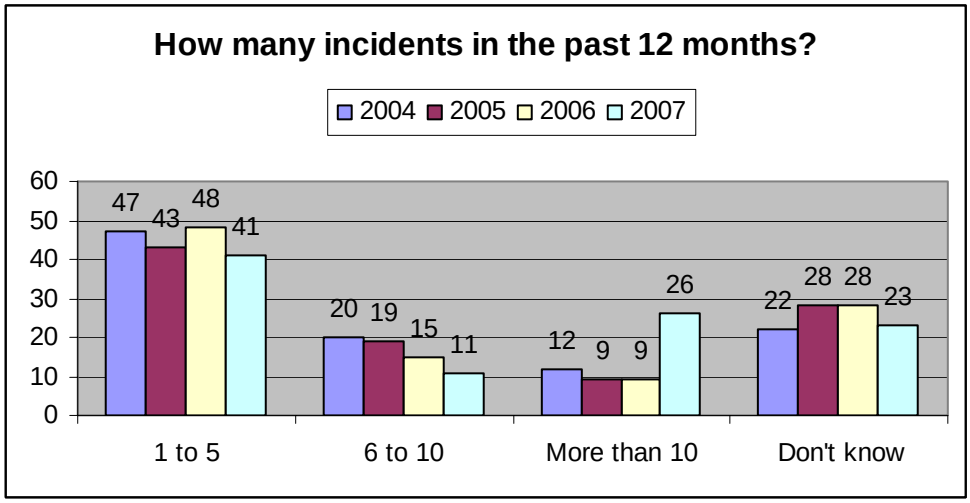
33% of enterprises surveyed believed a data breach can shut down their businesses and there is a good reason why. Breached are extremely costly in terms of money, but there is also the less tangible, but equally important cost to brand reputation. Based on the responses of 23 % of the respondents who could provide an estimate, the average cost of a data leakage incident was $1.82 million.

According to Deloitte,[111] the damage from breaches includes mostly direct financial costs (58%) with some exposure to internal costs (30%) and "reputational costs (12%) as well. 2007's damages are as follows:

- Less than 1M – 39%
- 1 to 5 M – 9%
- 6 to 10M – 3%
- 11 to 20M – 3%
- 21 to 49M – 4%
- Do not measure – 16%
- N/A have not experienced a financial loss – 26%

Most high-profile stories in the media today address the type of data loss that affects people on a personal level. Identity theft takes a toll on economies worldwide. In the UK, the Home Office estimates the cost of identity theft at $3.2 billion during the last three years. And while the costs are high for the individual, breaches involving customer's personal information are even more financially damaging for enterprises. On average, companies spend $268.000 just to inform their customers when such disasters occur.

The CSI Survey 2007[112] claims that, even though average losses are markedly up, computer security incidents occur with less frequency within organizations:

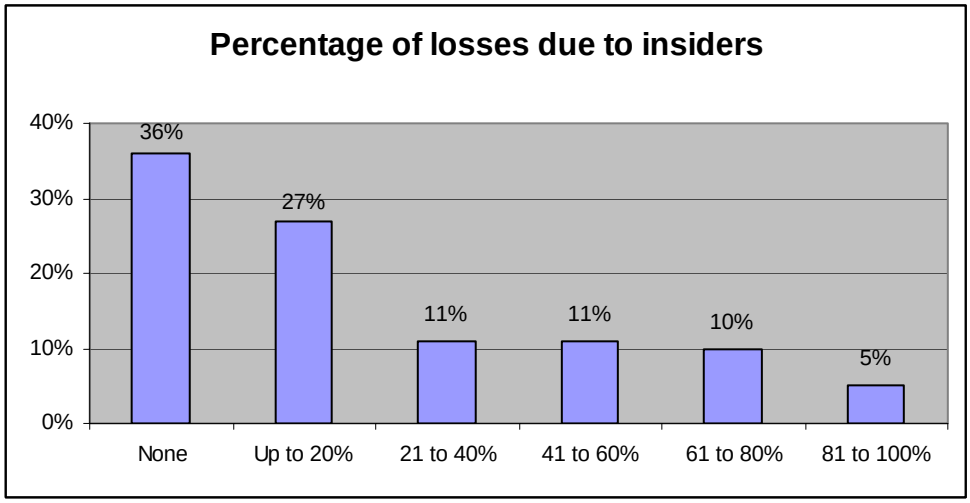


111 2007 Global Security Survey, Deloitte

112 http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

When respondents were asked straightforwardly whether anything amiss had occurred – other than quick network scans that may or may not signal an attack – only 46% said that they have. This figure is down from 52% in 2006 and 56% the year before. Overall, this is down from a peak of 70% in 2000.

Respondents attributed a high percentage of losses to insiders. As can be seen in the figure, slightly more than one-third (36%) of respondents believe that insider threats account for none of their organization's cyber losses—this is up from 32% last year.



Source: 2007 Global Security Survey

- **Negligence of employees, insider fraud, poor business processes and computer theft**

Prevention requires more than adopting heightened technological standards. Many security breaches result from negligence of employees, insider fraud, and poor business processes relating to information security.[113] Security professionals consider employee negligence and broken business processes much more acute threats to the security of confidential data than hackers. Two of the most highly publicized breaches, Choicepoint and the U.S. Department of Veterans Affairs, were not the result of a lack of technological protections so much as they were a result of poor business practices. Choicepoint failed to extend information security into customer validation processes, and the VA allowed an employee to take home a laptop containing millions of personally identified records. As data storage becomes more and more mobile, large amounts of confidential information become more easily accessible. Surveyed security professionals, in fact, acknowledge that it is very likely that PDAs, mobile devices, and laptops all contain unprotected sensitive or confidential information, and that is also likely that they would never be able to determine what actual sensitive data was stored on these devices in the event they were lost or stolen. What is even more disconcerting is that over 80% of these same respondents stated that their organization had suffered a loss or theft of one of these types of storage devices.

A survey done for UK businesses shows a decreasing trend for the levels of theft and fraud, with only one in twelve companies affected.[114] The most common type of theft

113 Security Breach Notification Laws: Views from Chief Security Officers
114

and fraud involving computers is the physical theft of computer equipment. The bigger the organisation, the more likely it is to have computer equipment stolen. Over a third of large businesses (and 82% of very large ones) reported theft of equipment by outsiders. Seven times as many firms suffered theft by outsiders as had thefts by their own staff. Large businesses have more thefts by staff, but even here it is still a three to one ratio.

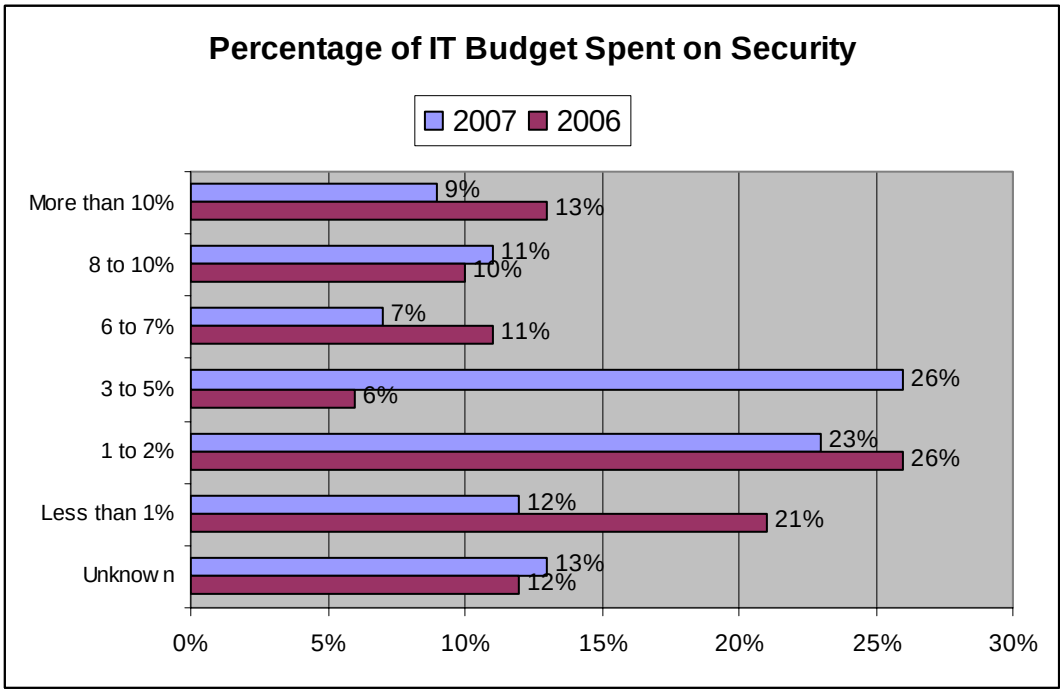
Instances of computer fraud were low. However, their impact on businesses is significant; several small businesses reported losses of between £10,000 and £50,000 as the result of computer assisted fraud. In larger businesses, some losses ran into millions. Four fifths of those affected by such incidents considered them serious, very serious or extremely serious. All of the organisations that had a computer fraud reported it as their worst security incident of the year.

3. IT SECURITY SPENDING/MEASURES

The very nature of "critical" information infrastructure is such that it needs to be secured as optimally as possible given the costs and benefits. The issue, however, is complicated because risks are difficult to estimate. Markets rely on information, but in this area, there is very little data about the probability of failures and their financial costs. In addition, investment in security is a strange insurance premium; the benefits (such as preventing incidents that would otherwise have occured) are often invisible and, regardless of how much is spent, there is no guarantee of safety. Spending the right amount on information security is a great challenge for businesses. Over-expenditure reduces profitability, while under-investment can leave the business exposed.
This makes it difficult for firms to reach decisions on how to handle the matter, and for a "market" to form to address it. On the contrary, there is a perverse commercial incentive for firms to internalize the risks and costs. Competitive pressures increase the reluctance of companies to invest in avoiding the consequences of CII failures. Coupled with this is a big free-rider problem: if most firms invest to secure their systems, some players will capture the benefits without paying, and thus no one wants to pay. Taken together, the situation suggests a market failure for CII protection. [115]

The amount spent on information-technology security worldwide is around $100 billion annually, and is growing between 5% and 10%. Companies generally spend around 5% of their IT budget on security, according to the research firm IDC; 40% of IT managers rank it their top priority. [116]
The CSI 2007 Computer Crime and Security Survey finds that the majority of companies (61%) allocate 5% or less of their overall IT budget to information security.

[115] Ensuring and insuring CIIP
[116] Same source



- Source: CSI 2007 Computer Crime and Security Survey

According to IDC IT security spending – including hardware, software and services – will increase in 2008 to €12.5 billion (US$19.9 billion), up 17.3% over 2007's €10.6 billion. The growth rate is projected to decline over the next four years, down to 11.8% by 2012. (The study covered Austria, Belgium, Denmark, Finland, France, Greece, Germany, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the U.K.)

A survey based on UK companies[117] reveals that the number of companies with a formal security policy is steadily increasing. Almost every UK business makes use of external guidance or expertise to supplement its in-house security capability. The proportion of IT budget that UK companies spend on information security has risen significantly. Spending the right amount on information security continues to challenge UK businesses. The average UK company now spends 4-5% of its IT budget this way, and for 28% it consumes 6% or more of their IT budget. Large companies spend roughly 6-8%. Almost every organisation backs up its critical data and three-quarters store these backups offsite. Furthermore, 98% of businesses have anti-virus software, 80% update anti-virus signatures within a day and 88% install critical operating system patches within a week.

However, only 44% of the companies have carried out any security risk assessment; there is still a shortage of security qualified staff; only one in eight companies has any; three-fifths of UK businesses are still without an overall security policy, though a third of these have defined an acceptable usage policy for the Internet.

[117] Information security breaches survey 2006

Organisations tend to spend more on information security if they have experienced incidents. 67% of those that spend 6% or more on their IT budget had at least one security incident in the last year, compared with only 42% of those that spend 1% or less on security. In other words, those with incidents spend on average roughly 5% of their IT budget on security; those without spend a third less on average.

The survey further reveals the following problems:

- a quarter of UK businesses are not protected against spyware;
- only 1% have a comprehensive approach for identity management (authentication, access control and user provisioning);
- three-fifths of companies that allow remote access do not encrypt their transmissions, businesses that allow remote access are more likely to have their networks penetrated;
- three-fifths of companies do not block staff access to inappropriate web-sites and only one in six scans outgoing e-mail for inappropriate content;
- 30% of transactional web-sites do not encrypt the transactions that pass over the Internet;
- one in five wireless networks is completely unprotected, while a further one in five is not encrypted;
- 55% of firms have taken no steps to protect themselves against the threat posed by removable media devices (e.g. USB tokens);
- two-fifths of companies that allow instant messaging have no controls in place over its use; only half of the companies that have implemented Voice over IP telephony evaluated the security risks before doing so.

The 2007 security survey done by Deloitte[118] for the EMEA (Europe, Middle East and Asia) countries reveals that the majority of EMEA respondents (82%) feel that security has risen as a critical are of business. The majority (82%) also feel that government driven security regulations are effective in improving the security posture in their industry. 77% say that they have both the commitment and funding to meet government-driven regulations. A large proportion of respondents have a security strategy (61%).

When asked about their organisation's security model structure, 73% have a centralised model while far fewer – 10% and 12% - have decentralised and federated models, respectively. The data clearly shows **support for a company-wide effort regarding security measures**.

When asked to what extent requirements related to security are burdensome, companies in most EU countries find them burdensome, according to the World Economic Forum Executive Opinion Survey 2006-2007:

[118] 2007 Global Security Survey, Deloitte

Complying with administrative requirements (permits regulations reporting) issued by the government in your country is (1 = burdensome 7 = not burdensome)

Rank	Country	Score
4	Finland	4.62
10	Estonia	4.31
11	Switzerland	4.28
21	Luxembourg	3.90
23	Denmark	3.88
28	Austria	3.68
29	Norway	3.65
34	Ireland	3.58
43	Lithuania	3.48
44	Romania	3.47
52	Slovenia	3.24
53	Sweden	3.23
54	Netherlands	3.22
55	Latvia	3.20
57	United Kingdom	3.16
59	Spain	3.14
61	Portugal	3.13
66	Germany	3.05
93	Belgium	2.78
94	Poland	2.77
95	Malta	2.72
96	Benin	2.72
97	Libya	2.70
106	Greece	2.60
107	Hungary	2.59
111	France	2.57
119	Czech Republic	2.36
124	Italy	2.12

Global Information Technology Report 2007-2008 (based on Source: World Economic Forum Executive Opinion Survey 2006 2007)

4. COSTS FOR THE VARIOUS MARKET PLAYERS

a. Individual consumers

The costs to individual consumers are difficult to measure, however they are likely significant. They may result in direct damages to hardware and software as well as financial and other damages due to identity theft or other fraudulent schemes. One example is the United States where consumers paid as much USD 7.8 billion over two years to repair or replace information systems infected with viruses and spyware.[118] While most of this data is not comparable across studies and the surveys are often limited in scope, it does illustrate the magnitude of the financial impact, for both businesses and consumers, resulting from malware.[119]

Based on information collected from 2,000 participants in its 2006 State of the Net survey, Consumer Reports projected total losses for US consumers of US$ 7.1 billion. One in five consumers reported problems with viruses, causing costs of US$ 3.3 billion. Fixing problems caused by spyware cost consumers US$ 1.7 billion and losses from phishing attacks amounted to US$ 3.1 billion.[120] The total damage in 2006 was down from the estimated US$ 8.4 billion in 2005.

Another estimate for the U.S. aimed at quantifying the direct damages to repair or replace information systems infected with viruses and spyware. According to the report, consumers paid nearly US$ 7.5 billion over two years to repair or replace hardware.[121]

b. Backbone and Internet Service Providers (BSPs and ISPs)

Both the costs and revenues of ISPs and hence their profitability are affected directly and indirectly by malware. The most immediate cost of malware is customer support and abuse management. These costs may rise further when the ISPs are impacted by blacklists trying to fight infected machines on their network. Forms of malware that increase traffic volume, such as botnets generating massive amounts of spam, if left uncontrolled, cause opportunity costs to the ISP. The level of these opportunity costs depends on the capacity utilisation of the existing network. If the network has significant spare capacity, the opportunity costs of additional traffic to the ISP will be low. However, if the network is near capacity utilisation, the opportunity costs may be significant as incremental malware-induced traffic may crowd out other traffic in the short run and require additional investment in network facilities, in particular routers and transmission capacity, in the medium and long run. Malware may also affect an ISP indirectly via reduced revenues if its brand name or customer reputation suffers, for example, because of blacklisting and reduced connectivity. ISPs will invest in preventative measures reducing malware, such as filters for incoming traffic or technology that enable them to quarantine infected customers, only if the cost is less than the direct and indirect cost inflicted by malware.[122]

---

119 Brendler, Beau (2007) (Souce: StopBadware Project).

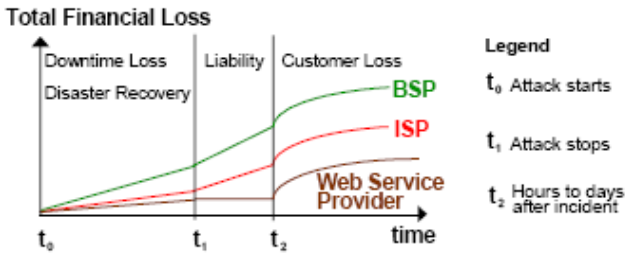
120 Consumer Reports, September 2007, pp. 30-31, http://www.Consumerreports.org

121 Consumer Reports, national survey 2006, http://www.Consumerreports.org

122 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

A study on the impact of large scale Internet attacks in Switzerland[123] estimates the loss for this type of company in the following way:

Loss of a BSP, an ISP and a web service provider



During the downtime [*t*0, *t*1] employee productivity is low due to Internet related services such as e-mail and web based communication no longer being available. Branch offices connected through virtual private networks (VPNs) are disconnected. If a BSP or ISP offers hosting or interconnection with pricing based on data transfer volume or if revenue is earned by showing ads on, e.g., a portal web site, financial loss corresponding to the service fees lost will be suffered. Productivity and revenue loss sum up to the *downtime loss*, which grows linearly with the length of the downtime. *Disaster recovery* mainly consists of additional work hours of network operators and grows linearly as well.

BSPs are hit stronger by *liability* claims than ISPs as unsatisfied customers of a BSP can often refer to an SLA and claim compensation.

Best-effort guarantees common for ISPs help to reduce such claims. However, a partial reimbursement of paid flat fees might occur.

As unhappy customers cannot immediately cancel a contract, the damage resulting from *customer loss* might occur weeks or even months after the actual technical incident. A sudden surge of customers terminating their contracts is likely to happen at the end of the current service period.

For the web service provider and backbone service provider sample scenarios given in the following table, the estimate precision is around ±30% of the given total damage.

[123] "Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks", A dissertation submitted to the Swiss Federal Institute of Technology, Thomas P. Dubendorfer

0	Factor	Symbol	Unit	BSP	WSP
Outage parameters					
	Outage time		h	24	168
	Working hours overlapping outage time	d_o	h	8	40
	Service operating time affected by outage	ds_o	h	24	168
	Degree of service degradation	S_o		100%	100%
Downtime Loss					
	Degraded Productivity				
1	Annual cost per employee	E_{ca}	CHF/yr	98,075	98,075
2	Working time per employee and year	d_a	h/yr	1,880	1,880
3	Employees affected by outage	E_{no}		3,500	4
4	Productivity degradation during outage	E_{po}		20%	20%
5	**SUM**		**CHF**	**292,128**	**1,669**
	Loss of Revenue				
6	Total annual revenue	R_a	CHF/yr	2,815 mill.	1,000,000
7	Service operating hours per year	ds_a	h	8,760	8,760
8	Part of the revenue affected by full outage	R_o		0%	0%
9	**SUM**		**CHF**	**0**	**0**
10	**SUM for Downtime**	L_D	**CHF**	**292,128**	**1,669**
Disaster Recovery					
10	Number of recovery team members	E_r		1,750 (50%)	0
11	Hourly cost for a recovery team member	E_{ch}	CHF	150	150
12	Recovery work outside office hours	d_r	h	16	0
13	Cost of material needed	M_c	CHF	1,000,000	0
14	**SUM for Recovery**	L_r	**CHF**	**5,200,000**	**0**
Liability					
15	Claims from contractual penalties	C_c	CHF	15,000,000	0
16	Claims from other liabilities	C_l	CHF	0	0
17	**SUM for Liability**	L_C	**CHF**	**15,000,000**	**0**
Customer Loss					
18	Time span	Δt	yrs	1	1
19	Number of actual customers lost	C_A		20	100
20	Number of potential customers lost	C_P		5	30
21	Average revenue per customer	R_C	CHF/yr	500,000	1,300
22	**SUM for Customer Loss**	L_{CL}	**CHF**	**12,500,000**	**169,000**
	Total Economic Loss (ca. $\pm 30\%$)		**CHF**	**32.99 mill.**	**0.17 mill.**

Comments (for table rows indicated):

0 BSP: Backbone Service Provider; WSP: Web Service Provider
1 Source: Swiss federal office for statistics [19, 20]
2 40 hours week and 5 weeks of vacations per year
4 Computer based work limited, no e-mail, no Internet
6 WSP: 6 employees, 800 customers, 2500 domains, CHF 1 mill. annual revenue
9 WSP: Assumes a flat rate for the data volume
10 WSP: Recovery is not a responsibility of the WSP

c. Web Service Providers

Web service providers often charge customers for their data transfer volume like ISPs do. The total loss due to *downtime*, *disaster recovery*, and *liability* is analogous in its characteristics to the ISP described above[124].

The damage due to *customer loss* depends heavily on the type of hosted customers. Infrequent and short interruptions will rarely be noticed by private customers, whereas e-shops can suffer a significant loss. A worst case would occur, if the web service provider's servers get broken into due to a lack of security, which would unsettle many customers.

[124] "Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks", Thomas P. Dubendorfer

In the case of a one week complete interruption of Internet dependent services, the study estimates that a WSP with 6 employees hosting 2500 domains of 800 customers and having CHF 1 mill. in annual revenue would suffer an estimated loss of CHF 0.17 mill.

d. Software vendors

Software vendors are affected in direct and indirect ways by malware. Malware uses vulnerabilities in their products to infect machines. The damage resulting from these vulnerabilities does not impact the software vendors directly, though it may have reputation effects and require costly response measures. Developing, testing and applying vulnerability patches is costly, not only on the part of the vendor, but also for its customers. Software developers typically face difficult development trade-offs between security, openness of software as a platform, user friendliness, and development costs. Investments in security may delay time to market and hence have additional opportunity cost in the form of lost first-mover advantages. On the other hand, if reputation affects work, software vendors whose products have a reputation of poor security may experience costs in the form of lost revenues. These effects are mitigated, however, by the fact that many software markets tend to have dominant firms and thus lock-in customers to specific products[125].

e. Registrars

Registrars have become part of the security ecosystem. Their business practices and policies affect the costs of malware and of the criminal business models built around it. Registrars may derive additional revenues from domain name registrations, even if they are related to malware, but they do not incur any specific direct costs. Nonetheless, if their domains are associated with malicious activity, it may result in an increasing number of formal and informal abuse notifications. Dealing with such abuse notifications is costly, requiring registrars to commit and train staff. Suspending domains may also result in legal liabilities. Furthermore, many registrars may be ill-equipped to deal with malware deregistration requests. Malware domain de-registrations can be very complex to process compared to, for example, phishing domain de-registrations, which are normally a clear breach of trademark or copyright. Some experts report that registrar abuse handling teams will often cite insufficient evidence to process a de-registration request, although evidence sufficient for many incident response teams has been provided. Because of the risk of legal action where a legitimate domain would be incorrectly de-registered, registrars often prefer to support their customer rather than the complainant. One of the economic costs that registrars face is proving the identity of registrants. Certain domain spaces (.com.au, for example), require strict tests of company registration and eligibility for a name before it can be granted. Evidence suggests that these constraints have lowered fraudulent domain registrations in the .com.au space. [126]

---

[125] OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

[126] OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

f. E-commerce companies and other Internet-dependent companies

E-commerce companies are impacted by malware in a variety of ways.[127] Many have to deal with DDoS attacks, often requiring them to buy more costly services from their ISPs so as to protect the availability of their services. Furthermore, malware has been used to capture confidential customer data, such as the credit card information registered with customers' accounts with e-commerce companies. Some sophisticated forms of malware have been able to defeat the security measures of online banking sites that rely on so-called multi-factor authentication – *i.e.* on more than just user login credentials. Even if customer information does not immediately allow access to financial resources, it can be used to personalise phishing e–mails that try to trick customers into revealing financial information. There are also cases where the malware is located on the servers of e-commerce companies, which are unaware that their website hosts malicious content that is distributed to its visitors. Typically, it is the e-commerce customers themselves that are harmed, though directly or indirectly the e-commerce company may also be affected. Financial service providers often compensate damages for their customers. For other companies there can be reputation effects.

In an atempt to measure the effects of large-scale Internet attacks the following estimates are given for e-commerce companies and other large companies[128]:

Loss of a corporate customer

An e-shop that sells only over the Internet also suffers severe *revenue loss* as e-shop customers that cannot connect to this online shop can easily buy in another one, which is currently available. Large companies and corporations typically sell over various channels and hence suffer a lot less *revenue loss* in case of Internet interruption. The resulting *downtime cost* grows linearly. *Disaster recovery* costs are rather small as the prevalent technical problems are typically solved by the ISP or BSP.

Liability claims are rare to occur for short business interruptions as is shown in the diagram. However, if an e-shop sells strongly time dependent goods on behalf of others and under a service level agreement, e.g., tickets for events, then compensation payments for service unavailability might occur. For long-term interruptions such claims can become a major issue. The same is true regarding *customer loss*.

A widespread, prolonged Internet disruption will affect the financial performance of a typical large company through a variety of channels, including lost productivity, lost

127 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

128 "Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks", Thomas P. Dubendorfer

revenue, lost customers, potential liability costs and reconstitution costs. The Business Roundtable estimates the impact of a widespread Internet disruption on an average Business Roundtable company with two specific examples[129]:

- **Degraded Productivity –** the deployment and use of Internet technology can substantially raise the productivity either directly or indirectly – of employees in today's large, sophisticated businesses. The average Business Roundtable company has 62,500 employees, and if Internet downtime results in an average productivity loss of 10%, a one-month Internet disruption will result in an estimated **$27.9** million of lost productivity for such a company, based on average hourly wages of $18.62.
- **Lost Revenue –** many companies derive a significant portion of their revenues from online transactions, and a widespread Internet disruption corrupting data could have a substantial impact on sales by Internet-dependent businesses. For example, an average Business Roundtable company has annual revenues of $31 billion derives 10% of its revenues from Internet transactions. If 25% of these revenues are permanently lost and not replaced with a sale when the disruption has been resolved, the company's lost sales for one month will be estimated at $63.7 million.

According to the information security breaches survey done for UK businesses[130], 62% of UK companies had a security incident in the last year and the average cost of a UK company's worst security incident of the year was roughly £12,000 (up from £10,000 two years ago). Large businesses are more likely to have security incidents (87%) and their breaches tend to be more expensive (£90,000 on average for the worst incident). Overall, the cost of security breaches to UK plc is up by roughly 50% since two years ago, and is of the order of ten billion pounds per year.

For many firms, the impact that an incident has on their reputation may be more important than financial loss. Other indirect costs such as investigation and remediation time also need to be considered. *A very large technology company's worst security incident was when a competitor gained access to two key bid documents. While there was no direct financial loss (and only a few days of investigation time), the incident was very serious to the business since it had implications for the whole bid strategy.*

The biggest single impact of security breaches continues to be business disruption. Three-fifths of organisations' worst incidents caused some interruption. Of these, just over a half caused more than a day's disruption, with some companies reporting more than a month of problems. The most disruptive type of incident is an attack on a web-site or Internet gateway; when these attacks interrupt service, they tend now to cause major disruption to the business, illustrating how most businesses are increasingly dependent on the Internet. *One large firm had web-site problems that resulted in customers being unable to access the site for three days. The result was lost orders and, of greater concern, the possibility of lost customers.*

As a whole, worst incidents caused disruption to small businesses, interrupting service for 1-2 days at an average cost of £6,000-£12,000, whereas large businesses suffered

[129] Business Roundtable, "Internet Business Dependence Report", 2007
[130] Information security breaches survey 2007

average interruption of 1-2 days and an average cost of that interruption £50,000-£100,000.

The incident response costs for organisation include the indirect cost of staff time responding to the incident. Two-thirds of UK businesses are able to investigate and correct their worst incident with less than a man-day's effort. 97% of firms spent less than 10 man-days of investigation and remediation time on their worst incident. Although it is rare for any incident to require more than £10,000 to be spent on recovery, the very largest firms find it difficult to quantify the cash cost of recovery; 38% of them did not know how much cash had been spent.

Fraud or theft using computers tends to be the most costly type of incident. Such incidents often require technical and legal expertise which is not always readily available in-house, especially for small businesses. *A telecoms company had an extremely serious fraud involving several million pounds. It took more than 100 man-days and cost more than £500,000 to investigate. The company's contingency plans for this eventuality proved effective, the technical configuration was fixed to prevent any repeat, and the perpetrators were prosecuted.*

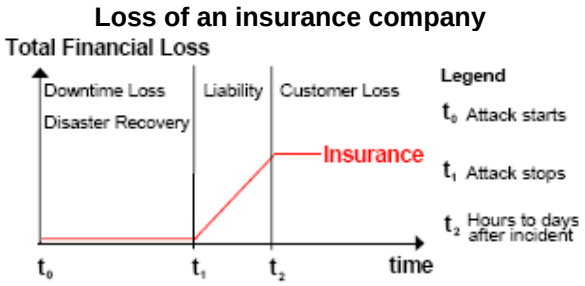
On average, UK businesses spent between £1,000 and £2,000 cash costs recovering from their worst incident. The average large firm spent £5,000 to £10,000.

A security breach may also cause direct financial loss. As well as loss of assets, direct costs may include fines imposed by regulators or compensation payments to customers. 2% of the surveyed UK firms had direct financial losses of over £10,000, half of these over £50,000. 4% of very large firms reported losses of more than £500,000 as a direct result of their worst incident.

The average total cost of a UK company's worst incident, based on these different impacts, is in the range of £8,000 to £17,000. For large businesses, the average cost is between £65,000 and £130,000. For very large respondents, the average cost of the worst incident is correspondingly greater, averaging roughly £1 million, with business disruption the largest component.

g. Insurance companies

Use of modern communication technologies such as the Internet to enhance a company's productivity are inevitable. However, many companies just slowly become aware that their financial success heavily depends on an "always-on" Internet. Traditional insurance policies such as corporate liability policies are not adequate to protect a company from business interruptions, productivity degradation and financial loss caused by Internet attacks.



The damage suffered by insurance companies in the event of a largescale Internet attack is mainly the sum of *liability* claims from insurance policies. The graph in Figure 2.4 does not show the comparably small *productivity loss* incurred[131].

h. Telcos

The Swiss study mentioned above[132] claims that as telephone networks, which generate the biggest part of the revenue for a telco, are usually separate from the Internet infrastructure, a telco suffers primarily from *productivity loss* of its employees that can no longer use the Internet during an attack. It is possible that a telco generates additional revenue during an attack due to people calling others by phone instead of sending e-mails.

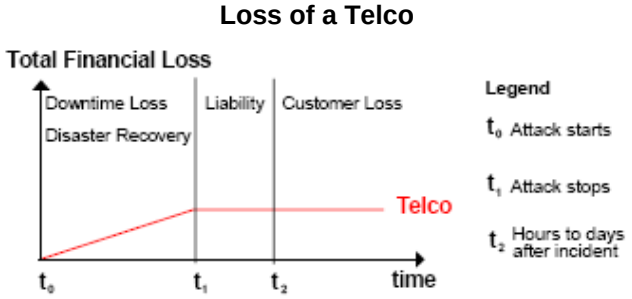


Figure 2.5: *Loss of a telco*

i. Banks

One association of banks in the United Kingdom estimated the direct losses caused by *malware* to its member organisations[133] at GBP 12.2 M in 2004, GBP 23.2 M in 2005, and GBP 33.5 M in 2006, an increase of 90% from 2004 and 44% from 2005. These direct losses are event not fully representative of the actual financial impact as they do not measure diminished customer trust in online transactions, loss in reputation, impact on the brand, and other indirect and opportunity costs that are challenging to quantify. Likewise, they do not include costs such as labour expenses for analysing malware, repairing, and cleansing infected machines, costs associated with the procurement of security tools (such as anti-virus and anti-malware software), or loss of productivity

131 "Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks", Thomas P. Dubendorfer
132 Same source
133 Whittaker, Colin (2007)

caused by the inability of employees to interact with a system when affected by an attack.[134]

j. Stock listed companies

Investigations into the stock price impact of cyber-attacks show that identified target firms suffer losses of 1%-5% in the days after an attack.[135] For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between $50 million and $200 million.

Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks).

Cavusoglu, et. al., examined 66 distinct security breaches that occurred between 1996 and 2001, 34 of which were DoS attacks. Of the 66 events, 31 affected firms whose business was conducted almost entirely over the Internet. The study found that firm value was negatively affected by Internet security breaches. Firms affected by the attack experienced a 2.1% decline in value, relative to unaffected firms. Furthermore, firms that rely on the Internet for conducting business were more affected than were more conventional firms. Internet firms affected by an attack experienced a 2.8% decline in value relative to the other firms that were studied. Smaller firms tended to lose more than did larger firms as the result of an attack. kind of attack seemed to make no significant difference. A DoS attack was not found to be any less costly than an attack where there was a more severe breach in security.

Ettredge and Richardson examined the effects of DoS attacks against Internet firms that occurred in February 2002. This study examined the behavior of the stock prices of over 100 Internet-only firms, during a three-day window centered on the day of the DoS attack in order to analyse if the costs of an attack were greater for those firms that had a greater dependence on the Internet. They found that, on average, as a result of the February 2002 attack Internet firms lost 5% more in market value than did non-Internet firms, immediately following the attack.

Garg, et. al., studied 22 events that occurred between 1996 and 2002.5 The authors determined that as a result of those attacks, the affected firms experienced a 2.7% decline in their stock price relative to the overall market on the day following the attack. Three days after the attack the stock prices of the affected firms had dropped 4.5%, relative to the rest of the market.The attacks were divided into four distinct types: simple web site defacing; DoS; theft of credit card information; and theft of other customer information. In the case of web site defacing, the average loss in stock value was 2% on the second day, which rebounded somewhat to a 1.1% loss on the third day. DoS attacks resulted in a 2.9% drop on the second day, and a 3.6% decline on the third day. For attacks that compromise non-financial information, there was an average drop in stock value of 0.5% on the day of the attack, and a total decline of 1.5% on the third day. Attacks which compromised financial information, chiefly credit card data, caused

134 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

135 Information based on “The Economic Impact of Cyber-Attacks”

the largest declines. On the day of the attack, stock prices of affected firms fell a average of 9.3% and by the third day the decline reached 15%. The authors also found that there was a correlation between the number of credit cards that were compromised and the magnitude of the stock price hit.

All the studies found that there was a significant decline in stock prices of affected firms in the days immediately following a cyber-attack. How significant are these percentage drops in dollar terms? At the end of 2003, the average market capitalization (stock price times number of shares outstanding) for a company listed on the New York Stock Exchange (NYSE) was about $4.4 billion; for a company traded on Nasdaq, it was $870 million. A 2% drop in market capitalization is equivalent to an average dollar loss of about $88 million for an NYSE firm and about $17 million for a Nasdaq company.

k. Governments

Society's heavy reliance on information systems makes the consequences of the failure or compromise of those systems potentially serious. Malware is an effective and efficient means for attackers to compromise large numbers of information systems, which cumulatively has the potential to undermine and erode society's ability to trust the integrity and confidentiality of information traversing these systems. The failure to provide adequate protection for the confidentiality and integrity of online transactions may have implications for governments. For example, electronic government (e-government) services, such as online filing for taxes or benefits, are likely to include personal data that if compromised could be used to commit fraud.

l. Risks to critical information infrastructures

Critical infrastructures at the basis of our society, such as power grids or water plants, are now often dependent upon the functioning of underlying IP-based networks for their instrumentation and control.[136] Most industrial control systems that both monitor and control critical processes were not designed with security in mind, let alone for a globally networked environment, but are now increasingly being connected, directly or indirectly (through corporate networks), to the Internet and therefore face a new set of threats. As these systems become based on more open standards - using Ethernet, TCP/IP and web technologies - they become vulnerable to the same security threats that exist for other information systems.

Thus, the disruption of critical information infrastructure systems through malware has the potential to impact the public and private sectors and society as a whole.

There have been a few cases where attacks using malware have directly or indirectly affected critical information infrastructure. For example, in Russia, malicious hackers used a trojan to take control of a gas pipeline run by Gazprom[137]. In January 2003 the "Slammer" worm, which caused major problems for IT systems around the world, penetrated the safety monitoring system at a US nuclear plant for nearly five hours. The US Nuclear Regulatory Commission investigated the incident and found that a

[136] OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL

[137] Denning, Dorothy (2000).

contractor established an unprotected computer connection to its corporate network, through which the worm successfully infected the plant network. More recently, the United States indicted James Brewer for operating a botnet of over 10,000 computers across the world, including computers located at Cook County Bureau of Health Services (CCBHS). The malware caused the infected computers to, among other things, repeatedly freeze or reboot without notice, thereby causing significant delays in the provision of medical services and access to data by CCBHS staff.

Although governments are often reluctant to disclose instances of attack against the critical infrastructure, it is apparent that protecting the information systems that support the critical infrastructure has become exceedingly important. Despite only a few reported cases, it is widely understood that critical information systems are vulnerable to attack. For example, although the 2003 blackout in the northeast US and Canada was attributed to a software failure, analysis of the incident demonstrated that the systems were vulnerable to electronic attack, including through the use of malware.

m. Macroeconomic consequences

The growing dependence on the Internet for business functions — in conjunction with the risk of terrorist attacks on the Internet infrastructure, as well as the consequences of natural disasters — raises well-founded concerns about the business impact and the costs to the economy and national security[138].

The World Economic Forum, estimates the global economic cost of an incident at approximately $250 billion.

Research conducted for Business Roundtable by Keybridge Associates[139] suggests that the economic costs of a month-long Internet disruption to the United States alone could be more than $200 billion.

Furthermore, a study by Dartmouth's Glassmeyer/McNamee Center for Digital Strategies and University of Virginia's School of Engineering and Applied Science looked at the economic costs of an Internet disruption to three industries. This study estimated that the costs of a 10-day event would be $22.6 million on the electrical parts sector, $54.15 million on the automobile parts sector and $404.76 million on the oil refining sector's Supervisory Control and Data Acquisition (SCADA) safety network.

An estimation of the macroeconomic costs for Switzerland in case of a major disruption lies on the following assumptions: 48.2% of all 3,590,000 employees working in Switzerland do an IT intense job. This results in 1,730,380 employees affected by a massive DDoS attack that causes an Internet blackout and that lasts one week (168 hours). The economic damage of such an event to the Swiss economy with an annual GDP of CHF 482 billion sums up to CHF 6 billion, i.e. 1.2% of GDP. For an Internet outage of a single working day the Swiss national scenario assumes that only 60% respectively 1,038,228 (i.e. all large enterprises and a part of the SMEs) of all employees in IT intense jobs are affected. In addition, the Swiss national scenarios do not account liability claims and loss of customers since it is assumed that liability is within Switzerland and no customers are lost.

[138] Business Roundtable, Internet Business Dependence Report, 2007

[139] Business Roundtable, Internet Business Dependence Report, 2007

National economic damage scenarios for Switzerland

0	Factor	Symbol	Unit	Swiss National Scenarios	
Outage parameters					
	Outage time		h	24	168
	Working hours overlapping outage time	d_o	h	8	40
	Service operating time affected by outage	ds_o	h	24	168
	Degree of service degradation	S_o		100%	100%
Downtime Loss					
	Degraded Productivity				
1	Annual cost per employee	E_{ca}	CHF/yr	98,075	98,075
2	Working time per employee and year	d_a	h/yr	1,880	1,880
3	Employees affected by outage	E_{no}		1,038,228	1,730,380
4	Productivity degradation during outage	E_{po}		20%	50%
5	**SUM**		**CHF**	**86,658,903**	**1,805,393,814**
	Loss of Revenue				
6	Total annual revenue	R_a	CHF/yr	482,000 mill.	482,000 mill.
7	Service operating hours per year	ds_a	h	8,760	8,760
8	Part of the revenue affected by full outage	R_o		15%	40%
9	**SUM**		**CHF**	**198,082,192**	**3,697,534,247**
10	**SUM for Downtime**	L_D	**CHF**	**284,741,095**	**5,502,928,061**
Disaster Recovery					
10	Number of employees in the recovery team	E_r		10,382 (1%)	17,304 (1%)
11	Cost per hour for a recovery team member	E_{ch}	CHF	150	150
12	Recovery work hours outside office hours	d_r	h	16	128
13	Cost of material needed	M_c	CHF	0	0
14	**SUM for Recovery**	L_r	**CHF**	**24,917,472**	**332,232,960**
Liability					
15	Claims from contractual penalties	C_c	CHF	0	0
16	Claims from other liabilities	C_l	CHF	0	0
17	**SUM for Liability**	L_C	**CHF**	**0**	**0**
Customer Loss					
18	Time span	Δt	yrs	0	0
19	Number of actual customers lost	C_A		0	0
20	Number of potential customers lost	C_P		0	0
21	Average revenue per customer	R_C	CHF/yr	0	0
22	**SUM for Customer Loss**	L_{CL}	**CHF**	**0**	**0**
	Total Economic Loss (ca. ±20%)		**CHF**	**309.66 mill.**	**5.84 bill.**

Comments (for table rows indicated):

1 Source: Swiss federal office for statistics [19, 20]
2 40 hours week and 5 weeks of vacations per year
4 Computer based work limited, no e-mail, no Internet
6 Source: Swiss federal office for statistics [18], Credit Suisse [38]
17 Claims only within Switzerland
22 No customers are lost

Another study, focused on the US[140], tries to find out what the macroeconomic effects would be if somehow a cyber-attack were able to disable some or all of the nation's network of computers. It tries to put things into perspective by examining previous events that have been labeled "disasters," and looking at estimates of the economic costs associated with them. It also acknowledges that there is a fundamental difference between a cyber-attack and a conventional physical attack in that a cyber-attack generally disables – rather than destroys – the target of the attack.

[140] The Economic Impact of Cyber-Attacks

It uses, among others, the electrical blackout of August 2003, as probably the most relevant to a consideration of the potential costs of a cyber-attack. Estimates of the cost of the blackout range from $6 to $10 billion for the entire U.S. economy, which accounted for 0.1% of GDP. The power failure imposed costs on both households and businesses. Production was disrupted, affecting earnings and profits, food stocks spoiled because of lack of refrigeration, and government costs rose because of the increased demand for police and other emergency services. The determinants of the cost of the power outage were principally the size of the area affected and the duration of the blackout. In the case of the power failure, there was little, if any, destruction of physical capital. The cost of the outage was primarily determined by its size and duration. Those two factors would likely also determine the economic cost of a cyber-attack.[68]

Any estimate of the potential economic cost of a cyber-attack must ultimately be speculative. Computers and other information processing equipment that might be vulnerable to attack make a direct contribution to the production of goods and services. But it is unclear how much other factors of production, both labor and capital, are dependent on computers. It seems within the realm of possibility that the effect of an attack on computers and their networks could have an effect on output much larger than that amount that is accounted for by their direct contribution. Electric power supplies might be affected. Banks might be unable to transfer funds.

The study argues that if all economic activity were to be temporarily interrupted by a cyber-attack, the only consideration in estimating the cost would be the duration of the event. The share of GDP produced on a given day is about 0.3% of the total for the entire year. Some of the production that might be interrupted is unlikely to be a permanent loss, but would simply be deferred until the effects of the attack dissipated. Since a considerable, if unknown, share of output is not dependent on computers, the final cost would be less than that. Historically, total annual production of goods and services has averaged roughly one-third of the value of the total stock of physical capital. As of 2001, computer equipment and software accounted for roughly 18% of the total capital stock. If equipment and software are assumed to contribute to output in the same way as other forms of capital, their direct contribution would account for about 18% of total annual production. If that share of output were interrupted for a single day it would amount to about 0.05% of total annual GDP.

The study concludes that as long as any cyber-attack is less than comprehensive and short-lived it is likely that any macroeconomic consequences will be fairly small. But, whatever the scope of the attack, the ability to recover quickly is important, since the length of time computers are affected is an important determinant of the costs. It may be almost as important for firms to address their abilities to restore operations as it is to work to insulate themselves from any potential attack.

5. BIBLIOGRAPHY

- *10th Annual Global Information Security Survey*, 2007 Ernst &Young
- *2007 Annual Study: U.S. Cost of a Data Breach*, Ponemon Institute, LLC
- *2007 Global Security Survey, The Shifting Security Paradigm*, Deloitte
- *2008 Information Security Breaches Survey*, The Department for Business, Enterprise & Regulatory Reform (BERR)
- *A Generic National Framework for CIIP, Center for Security Studies*, ETH Zurich
- *An Economic Damage Model for Large-Scale Internet Attacks*, Thomas Dubendorfer, Arno Wagner, Bernhard Plattner
- *Protection of Critical Infrastructures – Baseline Protection Concept*, Federal Ministry of the Interior, www.bmi.bund.de
- *Consumer Reports, September 2007*, pp. 30-31, http://www.Consumerreports.org
- *Critical information infrastructure: vulnerabilities, threats and responses*, 2007, Myriam Dunn Cavelty
- *Critical Infrastructure Protection: Elements of Risk*, 2007, George Mason University School of Law
- *Critical National Information Infrastructure – who owns it and how do we protect it*, http://www.bcs.org/upload/pdf/cnii.pdf
- *CSI Survey 2007, The 12th Annual Computer Crime and Security Survey*, Robert Richardson
- *Cyber Attack: A Risk Management Primer for CEOs and Directors, http://www.acus.org/docs/071212_Cyber_Attack_Report.pdf*
- *Datagate: The Next Inevitable Corporate Disaster?*, McAfee, http://www.mcafee.com/us/local_content/misc/dlp_datagate_research.pdf
- *DigiWorld Yearbook 2008, The Digital World's Challenges*
- *E-commerce and Cyber Crime: New Strategies for Managing the Risk of Exploitation*, KPMG
- *Ensuring (and Insuring?)Critical Information InfrastructureProtection*, Kenneth Cukier
- *Eurobarometer – E-Communications Household Survey (2006)*
- *Eurobarometer – Social values, science and technology (2005)*
- *Eurobarometer – Europeans, science and technology (2005)*
- *Eurobarometer – The European Emergency Number 112 (2008)*
- *E-Voting: International Developments and Lessons Learnt*, Buchsbaum, Thomas M., http://www.e-voting.cc/static/evoting/files/buchsbaum_p31-42.pdf

- *Examining the Feasibility of a Data Collection Framework*, 2007, Carsten Casper (ENISA), http://www.enisa.europa.eu/doc/pdf/studies/data_collection_report_20080214.pdf
- *Global Information Technology Report 2007-2008*, http://www.insead.edu/v1/gitr/wef/main/analysis/framework.cfm
- *Growing Business Dependence on the Internet*, 2007, Business Roundtable
- *High Tech Crimes Within the EU*, 2007, Europol, http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf
- *ICT security: e-Invoicing, and e-Payment Activities in European Enterprises, 2005*, E-Business Watch, http://www.ebusiness-watch.org/studies/special_topics/2005/documents/TR_2005_Payments_IV.pdf
- *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly
- *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues*, (TNO)
- *Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks, A dissertation submitted to the Swiss Federal Institute of Technology*, Thomas P. Dubendorfer
- *Irish Cybercrime Survey 2006: The impact of cybercrime on Irish Organisations*, ISSA/USD
- *Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organising National Cybersecurity Efforts, ITU Study Group Q22/1*
- *Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL*, OECD
- *Measurement of Trust In The Online Environment*, OECD
- *Measuring the Impacts if ICT Using Official Statistics*, OECD, http://www.oecd.org/dataoecd/43/25/39869939.pdf
- *Modelling eWork in Europe: Estimates, models and forecasts from the EMERGENCE project*, Bates P, Huws U. Report
- *Personal Internet Security*, UK House of Lords report, http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf
- *Practical Security Analysis of E-voting Systems, 2007*, Triinu Mägi, www.springerlink.com/index/p11qt87905582838.pdf
- *Reviews of Risk Management Policies: Norway - Information Security*, OECD
- *Scoping Study for the Measurement of the Trust in the Online Environment*, OECD
- *Security Breach Notification Laws: Views from Chief Security Officers, http://www.truststc.org/pubs/310/cso_study.pdf*

- *Security in Cyberspace: Combatting Distributed Denial of Service Attacks,* Jennifer A. Chandler, http://www.uoltj.ca/articles/vol1.1-2/2003-2004.1.1-2.uoltj.Chandler.231-261.pdf
- *Security Threat Report 2008,* Sophos
- *Surge in viruses and worms targeting mobile devices, satellite communications anticipated in 2005", 9 February 2005,* IBM, http://www-1.ibm.com/services/us/index.wss/rs/imc/a1008866
- *Symantec Global Internet Security Treat Report,* Trends for July-December 2007
- *The Economic Impact of Cyber-Attacks, 2004,* Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf
- *The EconomicIimpact of Regulatory Information Disclosure on Information Security Investments, Competition and Social Welfare,* Anindya Ghose, *http://weis2006.econinfosec.org/docs/37.pdf*
- *The European files, April 2008; Article: NIS Security: A constant challenge for ENISA*
- *The Top 20 Internet Security Vulnerabilities and How to Eliminate Them,* 2003, The SANS Institute, http://www.sans.org/top20/cdipresentation.pdf
- *Third Annual UK Online Fraud Report, 2007 Edition*
- *Virtual criminology report,* McAfee, http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf
- *Worldwide Infrastructure Security Report,* Arbor Networks
- http://www.eiaa.net/news/eiaa-articles-details.asp?id=158&lang=1
- http://db.e-voting.cc/europe
- http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf