OECD publishing

Please cite this paper as:

OECD (2012-11-16), "The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy", *OECD Digital Economy Papers*, No. 209, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5k8zq930xr5j-en

OECD Digital Economy Papers No. 209

The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy

OECD

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

16-Nov-2012

English - Or. English

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

Working Party on Information Security and Privacy

THE ROLE OF THE 2002 SECURITY GUIDELINES: TOWARDS CYBERSECURITY FOR AN OPEN AND INTERCONNECTED ECONOMY

JT03330872

DSTI/ICCP/REG(2012)8/FINAL
Unclassified

English - Or. English

FOREWORD

This paper was developed by the OECD Secretariat (Laurent Bernat, Directorate for Science, Technology and Industry, and Nick Mansfield, consultant to the OECD) in 2012, in the context of the second review of the 2002 Guidelines. It was circulated to delegations of the OECD Working Party on Information Security and Privacy (WPISP) as background to a questionnaire aimed at collecting their views regarding the continued relevance of the Guidelines and the potential need to revise them. It is expected to serve as a reference throughout the review process. It was declassified by the Committee for Information, Computer and Communications Policy (ICCP) at its 64th session on 24 October 2012.

This paper provides an overview of the history of the OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* ("Security Guidelines") since the adoption of their first version in 1992. In particular, it explains that the 2002 revision of the Guidelines introduced a fundamental paradigm shift in the way IT security was previously addressed, in order to take into account the emergence of the open Internet and the generalisation of interconnectivity. The 2002 Guidelines created a framework for security to remain effective in an open, dynamic and unpredictable technical environment where participants reduce risk before accepting it, instead of avoiding risk by limiting interconnectivity.

THE ROLE OF THE 2002 SECURITY GUIDELINES: TOWARDS CYBERSECURITY FOR AN OPEN AND INTERCONNECTED ECONOMY

A comparative analysis of a new generation of national cybersecurity strategies carried out by the OECD in 2012 highlighted that cybersecurity policy making has become a national priority in many countries.[1] This reflects key changes in the risk environment, with cyber threats evolving and increasing at a fast pace. The sources of threats have expanded along with their motivations and techniques. Malicious actors are better organised and more sophisticated. The priority now attached to cybersecurity also reflects the reality that the Internet and ICTs have become essential to economic and social development, forming a vital infrastructure. The new generation of cybersecurity strategies aims to drive economic and social prosperity and to protect cyberspace-reliant societies against cyber-threats while preserving the openness of the Internet as a platform for innovation and new sources of growth. While the stakes are now higher and the challenges greater, the fundamental approach required to combat cyber threats in an open and interconnected economy find its roots in the principles of the OECD's 2002 Guidelines.

Since 1992, the OECD has been addressing security as a fundamental requirement for information technologies to contribute to economic and social development. However, the paradigm that forms the basis of how security of information systems should be approached has evolved fundamentally over time. This brief history of the OECD *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* ("Security Guidelines") explains why the principles adopted in 2002 reflected a paradigm shift away from the way security of information systems was previously understood. Over the last ten years, these principles helped support the continued development of the Internet economy and benefitted all participants. They formed the basis for the development of national public policy frameworks by governments and were also used by public and private organisations as a foundation for the development of policies for the security of their own information systems and networks.

Although the Security Guidelines, like all OECD Recommendations,[2] are a non-binding instrument of the Organisation, they have a great moral force. They represent the political will of member countries and there is an expectation that member countries will do their utmost to fully implement them. Since the adoption of their first version in 1992, the Security Guidelines received strong support from OECD members and beyond. They served as a widely recognised international standard and helped the OECD to maintain its leadership in this policy area.

1. OECD, 2012a.

2. Recommendations are adopted in accordance to Article 5 of the Convention on the OECD which states that "In order to achieve its aims, the Organisation may: […] (b) make recommendations to Members; […]."

The 1992 Security Guidelines and their revision

OECD interest in the security of information systems dates back to 1988, when the Committee for Information, Computer and Communications Policy (ICCP) agreed to prepare a study on the security of information systems. Four years later, in November 1992, the OECD Council adopted a *Recommendation Concerning Guidelines for the Security of Information Systems* based on the recognition that "the increasingly significant role of information systems and growing dependence on them in national and international economies and trade and in social, cultural and political life call for special efforts to foster confidence in information systems" (OECD, 1992). The Guidelines were intended to provide a foundation from which countries and the private sector, acting singly and in concert, may construct a framework for the security of information systems.

The substantive core of the Recommendation consisted of an Annex with a "Principles" section including nine items (accountability, awareness, ethics, multidisciplinary, proportionality, integration, timeliness, reassessment, democracy) and an "Implementation" section with five items (policy development, education and training, enforcement and redress, exchange of information and co-operation). The Annex also included four other sections: Aims, Scope, Definitions, and Security Objectives. Following a set of recognising statements, the main part of the Recommendation included recommendations to member countries and called for a review of the instrument every five years. The Recommendation was accompanied by an explanatory memorandum.

A first review of the 1992 Guidelines was undertaken in 1997 by the ICCP Committee, through its Group of Experts on Information Security and Privacy (prior to being renamed Working Party on Information Security and Privacy (WPISP)), by means of a questionnaire issued to member countries. The review concluded that the 1992 Guidelines remained adequate to address the issues and purposes for which they had been formulated. However, it also recognised that since their publication, various other security issues and challenges had emerged, *e.g.* with regard to the increased connectivity between information systems, the related broadening scope of communication systems, and the emergence and use of the global information infrastructure (OECD, 1997).

The following review started in October 2000 and focused on "the development of inter-connected and interdependent information systems which are fundamental to modern economies" (OECD, 2000). An expert group was created to collect information on existing threats, vulnerabilities and actions taken by governments and the private sector. Japan offered to host a Workshop on Information Security in a Networked World in Tokyo on 12-13 September 2001 to exchange and share information, with a view to developing a common understanding of information security and enhancing OECD's involvement in this area (OECD, 2001a). A number of non-members participated including Brazil, China, Malaysia, Russia, South Africa and Thailand (OECD, 2001b).

This second review was marked by a sense of urgency which resulted from: *i)* the recognition that developments affecting the security of information systems in a world characterised by global ubiquitous networks significantly reduced the relevance of the 1992 Guidelines; and *ii)* the events of 11 September, which took place at the beginning of this process, the day before the Tokyo Workshop[3]. At the WPISP meeting following the Tokyo workshop, delegates agreed to form a new group of experts to revise the

3. See OECD, 2001b, p.5, Chairman's statement. See also the summary record of the WPISP meeting on 9-10 October 2001 (OECD, 2001c) where "delegates concurred that, particularly in light of the events of September 11, a thorough and expedited review should be conducted. In terms of the focus of the review, the majority of delegates emphasized the importance of ensuring the ongoing application of the Security Guidelines given the changing nature of information in a networked world and in considering the review in this context".

Guidelines. Over five months, this group met three times in Washington, Sydney and Paris to develop a first draft. In March 2002, WPISP delegates agreed with a proposal from the United States to expedite the review process for completion by early September 2002, building on the outcomes of three additional *ad hoc* WPISP meetings. On 25 July 2002, the OECD Council adopted new *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. As a consequence of the speed of the process, the revision was limited to the Principles and both the implementation section of the 1992 Guidelines and the explanatory memorandum were removed.

The 2002 Security Guidelines

As compared to their predecessor, the 2002 Security Guidelines reflect a fundamental change in the approach to the security of information systems which is the generalisation of interconnectedness.

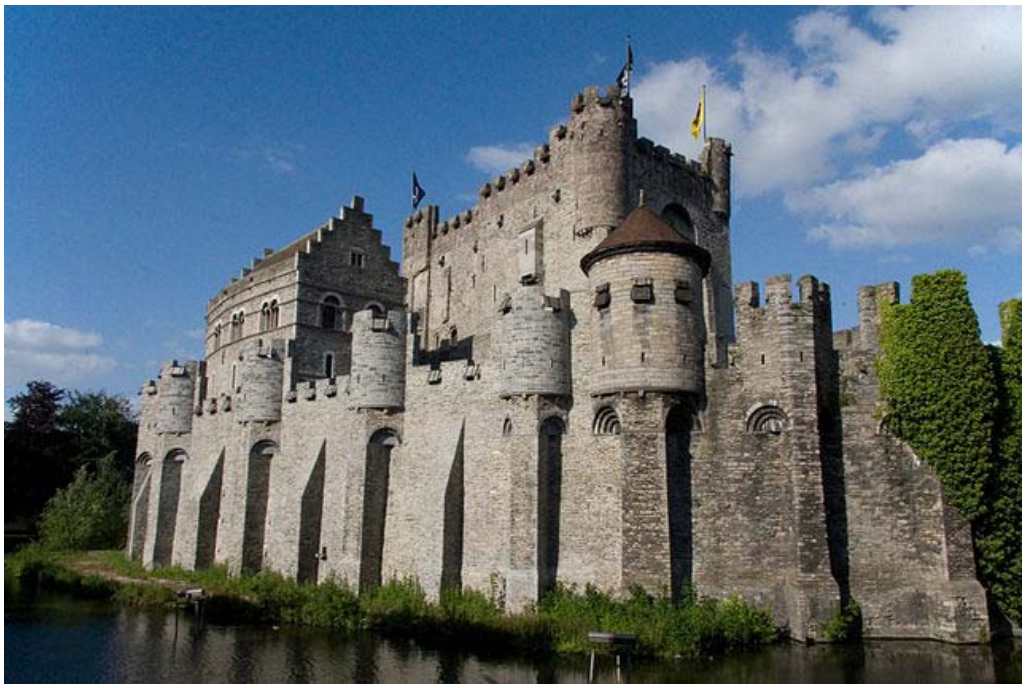
The 1990s security paradigm

In the early 1990s, information systems were operated in silo and did not interoperate easily. Security focused on internal threats. Protection against the outside world resulted from reinforcing the main characteristic of information systems: keeping them closed by default and opening them only by exception and under tight controls. It was the age of perimetre security, where the isolation of the system kept threats away and protected it by avoiding risk.

Twenty years ago, organisations' IT infrastructure typically consisted of multiple information systems operated in silos, in a closed and isolated manner. Systems were deployed to achieve specific purposes in various branches of an organisation, generally to increase productivity through "business automation". Although networked computing existed, in practice, different network protocols were used in different contexts within a single organisation and applications were not designed for the easy exchange of data with other applications. *A fortiori*, communication of these systems with other systems located outside the organisation was exceptional. Siloed information systems resulted from many factors, such as the heterogeneity of the technology, lack of basic compatibility or interoperability, imprecision of standards, independent implementation, as well as the corporate culture of that time.

The security paradigm that generally prevailed reflected this situation. The priority was to address internal threats such as technical failure or theft of information by an insider. External threats were not the most significant ones because IT environments did not provide many opportunities for their propagation. They were addressed by reinforcing an already existing state of relative isolation of the information systems from the outside world, prohibiting inbound and outbound flows of information by default unless specifically authorised, and placing any exceptionally authorised external flows under tight security control. This approach, which aimed to avoid external risk, was generally based on "perimeter security", and can be pictured metaphorically as the thick walls, high towers and deep moats that surrounded middle-age cities with few guarded gates and bridges. Thus systems were not closed because of security; rather computing was closed and siloed as a result of limited demand and technical opportunity for openness and interconnectedness. The security paradigm was simply aligned with this operational reality.

Figure 1. Metaphor: Security of Information Systems in 1992



Note: Gravensteen, Ghent, Belgium
Source: *http://en.wikipedia.org/wiki/File:Gravensteen_%28Gent%29_MM.jpg*

The emergence of interconnectedness

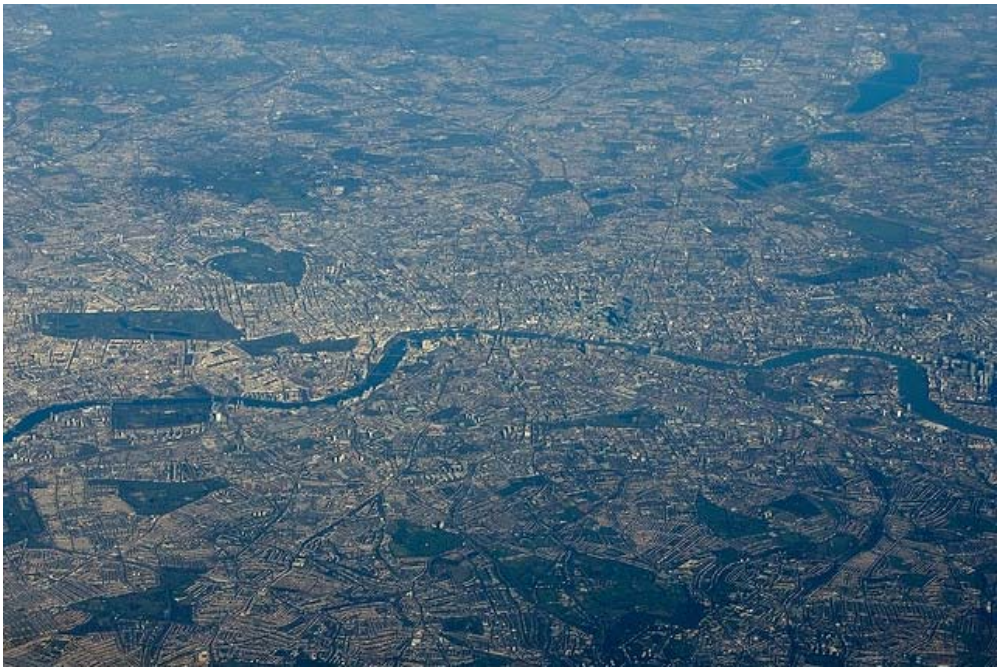
From the second part of the 1990s, the IT environment paradigm progressively evolved to network openness, enabled by the generalisation of Internet technologies which facilitated the interconnection of information systems. This evolution was mainly driven by the economic and social benefits of interconnectivity which generated an insatiable demand for increased information flows within and across organisations and even jurisdiction boundaries. In 2008, the OECD recognised the Internet Economy as a driver for economic growth, prosperity and improved quality of life.

The wide adoption of Internet technologies – the so-called layered TCP/IP network stack – unified network technologies and fostered networked communications both vertically within one organisation's subsystems and horizontally, across the information systems of different organisations. Seamless interoperability and interconnectivity enabled the various, previously siloed, IT components of organisations to morph into joined-up information systems, within which information could flow freely. Moreover, information flows could henceforth extend beyond the constraints of organisational boundaries, and even national borders and jurisdictions.

Progressively, network interoperability became available by default on every component of information systems, switching the IT environment paradigm from isolation to openness. However, while the technology certainly enabled this evolution, the **business benefits of interconnectivity** were the real driver of the strong demand for opening networks and enabling more information to flow within and across organisations. Over the course of a few years, generalised interconnectivity profoundly modified business operations by enabling, for example, real time supply chain management, just-in-time production strategies (JIT) and enterprise resource planning (ERP). Other, sometimes simpler, applications such as e-mail, voice and video conference, also transformed businesses and governments' activities. In parallel, ICT and

Internet penetration to households took off exponentially, connecting hundreds of millions of home, business and government users together across the Internet, forming a single global network of networks and enabling e-commerce, e-government and many other forms of digital interactions. Finally, progress in the technologies, liberalisation of telecommunication markets and increased bandwidth capacity, among other factors, fed an insatiable demand for more interconnectivity. The paradigm shift from closed networks to the open Internet gave birth to the Internet economy, a driver for economic growth, prosperity and quality of life, as recognised by the OECD in June 2008.[4]

Figure 2. Metaphor of the IT environment in 2002 and after



Note: London metropolitan area from above. Source: François Roche. http://www.flickr.com/photos/13066221@N03/2279144561/. Some rights reserved (CreativeCommons BY-NC-SA 2.0).

The metaphoric representation of information systems as isolated fortified cities of the early 1990s became outdated. Instead, a single global ecosystem formed by myriads of widely interconnected groups of subsystems emerged, changing the walled cities metaphor to one giant megalopolis with varied open districts in permanent contact and exchange with each other.

The impact of interconnectedness on the 1990s security paradigm

The growth of information assets and participants' reliance on the Internet attracted cybercrime, and external threats became the security priority for organisations…

As economic and social interactions migrated to the Internet, so did crime. The attractiveness of the digital world for criminals of all kinds increased with the value of the assets they could reach in that space and with the reliance of people and organisations on interconnected information systems. Unfortunately, as these threats increased, the effectiveness of security measures designed to protect a closed environment progressively diminished, creating ever more opportunities for external malicious actors. Although they

4 . OECD, 2008e.

remained present, internal threats lost the main focus of IT security and external threats, characterised by their **fast changing** nature, became the main priority.

… While, the security paradigm tailored to a closed, relatively static and predictable environment was increasingly ineffective in addressing the fast-evolving nature of threats, the growth of information flows, and the dynamism and instability of the new interconnected and opened environment.

The security paradigm designed for a closed environment was fundamentally challenged by network openness. The multiplication of entry/exit points in information systems undermined the principle of establishing security by keeping systems as much isolated as possible. With generalised interconnectedness, the volume of information flows increased by several orders of magnitude without any limit being set. A **scalability challenge** emerged as security controls designed for addressing limited information exchanges became less effective when applied to massive information flows. Moreover, as interconnectedness enabled new devices, new computer code and new usages to be constantly introduced in systems, the IT environment switched from static, stable, and predictable to dynamic, unstable and unpredictable. Each change in the environment was potentially creating a new vulnerability, ready for exploitation by malicious actors of various kinds. By introducing **instability** in the IT environment, interconnectedness made obsolete both security mechanisms tailored for a stable environment and the objective of creating a stable state of security within information systems.

Attracted by the benefits of interconnectivity, the economy and the society continued to migrate at a fast pace to the digital world, despite the inappropriateness of the IT security paradigm.

With varying degrees, depending on corporate cultures and contexts, tensions appeared between security requirements and business demand. From a security perspective, the evolution towards more openness in the name of potential business benefits was perceived as undermining the protection of organisations' assets. From a business perspective, however, security requirements which limited and controlled openness were perceived as an obstacle to harnessing the potential business benefits of interconnectedness.

Ultimately, the demand for interconnectivity and free flow of information across networks became such that perimeter security blocking information flows by default and enabling them by exception became untenable from a business perspective. Eventually, the IT operational paradigm switched from closed to open networks despite its fundamental contradiction with the then dominant security paradigm. A new security paradigm had to be introduced to realign security with the new reality of the operational environment.

The 2002 Security Guidelines: concepts for security in an open environment

In order to realign security with the new open and interconnected IT environment, the 2002 Security Guidelines shifted the security paradigm from static risk avoidance to dynamic risk management.

The 2002 Security Guidelines realigned security with the new digital environment, where the benefits of the free flow of information enabled by open and interconnected networks make it impossible to continue avoiding external risk by closing the system (so-called "perimeter security"). The Guidelines started from the premise that if the environment is open, information assets are going to be constantly exposed to a changing risk which cannot be totally eliminated, but can be managed and reduced before it is accepted. The Guidelines switched the paradigm of security of information systems and networks from risk

avoidance to risk management, where perimetre security is one among many other means for reducing risks. In so doing, they transposed the security reality of the physical world in the digital world.

The principles of the Guidelines create a framework for security in an open digital world where participants reduce risk before accepting it, instead of avoiding risk by limiting interconnectivity.

All the principles of the Guidelines flow from this logic. While within a closed system, security can be taken care of by the operator of the system without users having to think too much about it, managing risk in an open, dynamic, unnstable and uncertain environment requires awareness of all the participants. Everybody has to play a part to reduce this uncertainty because no central authority can control all the flows at the gates anymore: there are too many access points and information flows are too large and complex. All participants have some responsibility for security, according to their role (2. Responsibility), a responsibility that requires an increased level of awareness about the need for security (1. Awareness). Likewise, if there is uncertainty, then security incidents and emergencies will happen. Detecting and responding to them becomes vital to protect business operations (3. Response).

Furthermore, interconnected networks now form a single distributed (*i.e.* decentralised) network. All participants can be considered as part of a single society because they operate in a shared environment and are, to some degree, interdependent: the consequences of participants' actions in one part of the network are not blocked by the walls protecting another part anymore but rather actions flow across networks, and may harm others, just as they may benefit them. Therefore, participants' behaviours should take into account that the Internet is a shared environment where some social norms should be respected, for the benefit of all. Participants should respect the legitimate interests of others (4. Ethics) and those who implement security measures should do so in a manner that respects the values of a democratic society (5. Democracy). Social values shared by OECD countries in the physical world should be shared in the digital world as well.

Risk is the result of potential threats which can exploit vulnerabilities to cause detrimental consequences. Managing risk requires to first conduct risk assessments to identify these threats and vulnerabilities, and understand their potential detrimental impacts (6. Risk Assessment). Because all assets placed in the open environment will face some degree of risk, security should be a fundamental element of all products, services, systems and networks. Participants should incorporate security as an essential element of information systems and networks (7. Security design and implementation). They should also adopt a comprehensive approach to security management, encompassing all levels of participants' activities and all aspects of their operations (8. Security management).

Finally, because threats can originate from anywhere on a network which connects almost all systems across the globe, they continuously evolve in nature, intensity and characteristics. Organisations as well as technologies also evolve continuously, shaping an ever changing environment where new vulnerabilities appear all the time. Therefore participants should continually review, reassess and modify all aspects of security to deal with evolving risks. An open world is a dynamic world. This dynamism enables creativity and innovation for better and for worse. Therefore, security should not be static. Consistent with the nature of the environment, it should be dynamic (9. Reassessment).

The impact of the 2002 Security Guidelines

The 2002 Security Guidelines had a considerable impact. The press release announcing their adoption was widely disseminated and commented by the media and the Guidelines set the 2002 record of the "most downloaded document in one month" on the OECD web site. As part of their commitment to disseminate them, member and non-member countries volunteered to translate the Guidelines and several months later, they were available in Chinese, Hungarian, Italian, Norwegian, Polish, Russian, Slovak, Spanish, Swedish

and Turkish. The United Nations Resolution Concerning the Creation of a Global Culture of Cybersecurity (United Nations, 2002) reflected the nine principles of the Guidelines and invited "Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005". The Guidelines were also reflected in the European Council Resolution "on a European approach towards a culture of network and information security" (European Council, 2003) and in the Asia-Pacific "Strategy to Ensure Trusted, Secure and Sustainable Online Environment" (APEC, 2005).

After the adoption of the 2002 Guidelines

To complete the process for the development and adoption of the Guidelines over less than a year, delegates had agreed to focus on the Principles' section. As a result, the current Guidelines do not include a revised implementation section and the 1992 explanatory memorandum, which was never updated, became obsolete.

After 2002, the WPISP followed-up on the adoption of the Guidelines by pursing two different streams of activities, respectively between 2002 and 2005 and after 2005.

Immediately after 2002 and before 2005, the OECD focused on sharing experience and best practices across member and non-member countries, and on monitoring implementation of the Guidelines. The WPISP developed an implementation plan (OECD, 2003) and BIAC, with the International Chamber of Commerce (ICC), published an International Business Companion to the 2002 OECD Guidelines. The Secretariat developed a "Culture of Security" Web Site which included a list of national and international initiatives carried out by countries to implement the Guidelines. Norway hosted an OECD Global Forum on Information Systems and Networks Security (OECD, 2004a) with member and non-member economies, business and civil society to share information, take stock of progress made in national implementation, and discuss expanding the culture of security. The WPISP carried out two surveys on the implementation of the Security Guidelines (OECD, 2004b, 2005a) and held a workshop jointly with APEC in Seoul, Korea, to share information, experience and best practices to develop a culture of security (OECD, 2005b).

After 2005, the WPISP shifted its focus to specific areas of implementation of the Guidelines, such as Critical Information Infrastructures Protection (CIIP). A comparative analysis of national CIIP policies (OECD, 2008a) led to the adoption of a Council Recommendation in 2008 (OECD, 2008b). The working party also developed guidance on Radio-Frequency Identification which included security (OECD, 2008c). Malware (OECD, 2009) and more recently Proactive Measures by ISPs against Botnets (OECD, 2012b) were also addressed. Finally, a comparative analysis of national cybersecurity strategies was carried out (OECD, 2012a) to explore recent evolutions of public policies in this area and to feed into the 2012 review of the Security Guidelines.

The reviews of the Guidelines after 2002

In 2007, the Working Party reviewed the 2002 Security Guidelines by way of a questionnaire circulated to WPISP delegations (OECD, 2007a) to which only eleven countries responded. No consensus emerged on the need to revise the Guidelines at that stage. Potential new concepts that emerged in the discussions were related to implementation, such as interdependent information systems and networks, research and development, and enhanced international co-operation and collaboration (between regulatory agencies on the one hand and governments and the private sector on the other hand) in addressing threats to both the security of information systems and networks and the security of users of those systems. The

importance of taking into account the linkages between information security and privacy were also highlighted (OECD, 2008d).[5]

The second review of the 2002 Security Guidelines was initiated in 2012 by the WPISP (OECD, 2012c).

5. The absence of the concept of international co-operation in the Guidelines had previously been highlighted in a paper which mapped the findings of the work on Critical Information Infrastructure Protection Policy with the principles of the Security Guidelines (OECD, 2007b). The 2008 Council Recommendation on the Protection of Critical Information Infrastructure (OECD, 2008b) addresses both domestic and international policies.

REFERENCES

APEC (2005), APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment. Available at *www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx*

BIAC, ICC (2003), Information Security Assurance for Executives. An international business companion to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security. Available at *www.oecd.org/dataoecd/54/22/37019249.pdf*.

European Council (2003), Council Resolution on a European approach towards a culture of network and information security. Available at *www.oecd.org/dataoecd/53/59/37019852.pdf*.

OECD (1992), Recommendation of the Council Concerning Guidelines for the Security of Information Systems. Available at *www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_1,00.html*

OECD (1997), Review of the 1992 Guidelines for the Security of Information Systems. October 1997: Available at *www.oecd.org/fr/internet/economiedelinternet/2096313.pdf*.

OECD (2001b), Proceedings of the OECD Workshop: "Information Security in a Networked World". Available at *www.oecd.org/dataoecd/15/18/2387671.pdf*.

OECD (2002), Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, Available at *http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=116. See also www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html.*

OECD (2003), Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Available at *www.oecd.org/dataoecd/23/11/31670189.pdf.*

OECD (2004a), OECD Global Forum on Information Systems and Networks Security: Towards a Culture of Security. Proceedings. Available at *www.oecd.org/dataoecd/54/32/31453706.pdf*.

OECD (2004b), Summary of Responses to the Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Available at *www.oecd.org/officialdocuments/displaydocumentpdf?cote=dsti/iccp/reg%282003%298/final.*

OECD (2005a), The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries. Available at *http://oecd.org/dataoecd/16/27/35884541.pdf*.

OECD (2005b), OECD-APEC Workshop on Security of Information Systems and Networks - Seoul, 5-6 September 2005. Available at *http://oecd.org/document/25/0,3746,en_2649_34255_35481241_1_1_1_1,00.html*.

OECD (2007a), First Review of the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [DSTI/ICCP/REG(2007)19](Unclassified).

OECD (2007b), Preliminary Outcomes from WPISP Work on Security: Policies for the protection of critical information infrastructures (CII). Available at: *http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2012)4&docLanguage=En*

OECD (2008a), Development of Policies for Protection of Critical Information Infrastructures. Ministerial Background Report. Available at *www.oecd.org/dataoecd/1/13/40825404.pdf*.

OECD (2008b), OECD Recommendation of the Council on the Protection of Critical Information Infrastructures. Available at *www.oecd.org/dataoecd/1/13/40825404.pdf*.

OECD (2008c), RFID. OECD Policy Guidance. A Focus on Information Security and Privacy. Applications, Impacts and Country Initiatives. Available at www.oecd.org/dataoecd/19/42/40892347.pdf.

OECD (2008d), Report on the Review of the 2002 Guidelines on the Security of Information Systems and Networks. Available at: *http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2012)3&docLanguage=Fr*.

OECD (2008e), Declaration for the Future of the Internet Economy (The Seoul Declaration). Available at *www.oecd.org/dataoecd/49/28/40839436.pdf*.

OECD (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, OECD Publishing. doi: 10.1787/9789264056510-en

OECD (2012), "ICTs, the Internet and the crisis: Macro trends", in OECD, *OECD Internet Economy Outlook 2012*, OECD Publishing. doi: 10.1787/9789264086463-4-en

OECD (2012a), Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.

OECD (2012), "Proactive Policy Measures by Internet Service Providers against Botnets", *OECD Digital Economy Papers*, No. 199, OECD Publishing. doi: 10.1787/5k98tq42t18w-en

OECD (2012c), Terms of Reference for the Review of the OECD Guidelines for the Security of Information Systems and Networks

United Nations (2002), Resolution Concerning the Creation of a Global Culture of Cybersecurity, A/RES/57/239. Available at *www.oecd.org/dataoecd/53/60/37019786.pdf*