# OECD Studies in Risk Management

# Norway

## INFORMATION SECURITY

OECD

OECD STUDIES IN RISK MANAGEMENT

# Norway

## INFORMATION SECURITY

OECD
ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT

## Foreword

The OECD Futures Project on Risk Management Policies aims to assist OECD countries in identifying the challenges of managing risks in the 21st century, and contributing to their reflection on how best to address those challenges. Its focus is placed on the consistency of risk management policies and on their ability to deal with the challenges, present and future, created by systemic risks. It is designed in two phases. In Phase 1, the countries participating in the project propose specific themes as case studies of their risk management policies. For each proposal, the OECD Secretariat prepares an overview of the issue covering both recent international developments of interest and the national policy context. In addition, the Secretariat elaborates a tool for self-assessment and review, consisting of one or several questionnaires following the methodological framework of the project. This prepares the ground for Phase 2 in which an in-depth review of the risk management issues will be conducted by a team of experts for those countries that wish it. Self-assessments will be used as the basis of these reviews. At the end of phase 2, a cross-country report will bring together the lessons learned from the project, and identify opportunities for sharing best practices and improving risk management.

In the framework of the OECD Futures Project on Risk Management Policies, the Norwegian Ministry of Justice and the Police has proposed a Phase 1 case study on "an assessment of information and communication technology security measures with an aim to developing optimal broad-spectrum vulnerability reduction". The study would lay the ground for self-assessment and review of Norway's ICT security policies, with the objective, in the Ministry's words, of "aid(ing) national authorities and the new National Information Security Coordination Council (KIS) in refining and developing focussed (…) measures and policies aimed at reducing vulnerabilities".

In March 2004, the Directorate for Civil Protection and Emergency Preparedness (DSB), attached to the Ministry of Justice, organised a two-day workshop in Oslo, where it convened, in addition to the OECD Secretariat, a large number of actors involved in the management of information security. These included in particular the Ministry of Trade and Industry, then in charge of implementing the government's strategy regarding Information and Communication Technologies, the Ministry of Defence, and the National Security Authority. The workshop provided an overview of the Norwegian government's initiatives in the area of ICT security over the past years, and confirmed that there was strong interest for a first assessment of these measures. Information security is an emerging policy area, where novel institutional settings and public policy tools need to be tested for possible gaps and inconsistencies.

This study has been prepared by Reza Lahidji and Marit Undseth, from the OECD International Futures Programme. The authors have benefited from the support of Stein Henriksen and Hilde Bostrøm Lindland, at the Directorate for Civil Protection and Emergency Preparedness, and from the guidance of the Steering Group to the OECD Futures Project (see the list of Steering Group members in Annex 4). The study is issued under the responsibility of the Secretary General of the OECD.

## Table of contents

## Introduction

The development of information and communication technologies and networks, and in particular that of the Internet, has gone hand in hand with the emergence of new types of malevolent actions called cyber-crime: viruses, worms, Trojan horses, and the like. This study is about the threat that such acts represent for the secure functioning of information systems and networks, their costs and their implications for public policy. Its emphasis is therefore placed on deliberate, malicious acts and on security, leaving aside questions of safety.

As in many other areas, risk assessment and reduction in the field of information security can be conducted at both ends of the risk chain: hazards, i.e. cyber-threats, on one hand, and endpoints, i.e. exposed information systems and networks, on the other. The use of the word "cyber-crime" is sometimes dedicated to the first type of actions (threat assessment and reduction through the design and enforcement of law), while the second type is referred to as "cyber-security" (protection and resilience of target systems and networks). This study does not make such terminological distinctions, but refers explicitly to laws, regulations and policy measures. The scope of the study is limited to vulnerability reduction, but important events and initiatives in the field of threat reduction are also mentioned. Naturally, effective governmental (and international) action in the area of ICT security needs to address both aspects in a consistent manner.

The study is organised in three parts. The first part analyses why cyber-crime has become a real threat for OECD societies, paying particular attention to the dependence of critical infrastructures on IT systems. The second part discusses what governments can and should do about it, in conjunction with the private sector and civil society. It reviews in particular a number of recent policy initiatives in various OECD countries and at the international level. The third part describes the context in which Norwegian ICT security policy has evolved in recent years. The study concludes with a proposal for a self-assessment and review of related policies in Norway. Annex 1 to the study presents the Norwegian IT security management system following the project's methodological framework. Annex 2 contains a comprehensive list of the laws of interest for the case study. Annex 3 proposes a questionnaire, designed as a tool for self-assessment and review, for the second phase of the project. Members of the Steering Group to the Project are presented in Annex 4. The study also includes a technical glossary and a bibliography.

## The rise of cyber-threats

Threats to cyber-security range from relatively harmless intrusions to the disruption of critical information systems, through fraud, theft of sensitive information, and so on. More generally, the notion of cyber-crime encompasses any deliberate act affecting three fundamental properties of an information system:

- confidentiality, i.e. a computer system's or network's ability to store sensitive information in a secure manner and to maintain exclusive access to designated users;
- integrity, i.e. the assurance that programmes and data are designed and modified only in an authorised manner, and hence reliable;[1] and
- availability, i.e. continuous accessibility and service of the computer system or network to users without delays or blackouts.[2,3]

Such harmful acts can affect individual users, small and large corporations and governmental services, and generate a variety of costs:

- direct costs, such as the theft of money, digital assets, or sensitive information;
- indirect costs in the form of business interruption, legal liability, and lower productivity due to diverted resources (personnel, capital, bandwidth and computing power, etc.); and
- secondary costs related to the long-term impact of an attack on brand image, competitiveness, financial markets, etc.

Cyber-crime has considerably evolved over the years to become a real threat to society, due to four principal factors reviewed hereafter: attack tools have become much more sophisticated; new technologies have brought new vulnerabilities; critical infrastructures have become dependent on the security of information systems and networks; and finally, the scope of cyber-crime has considerably increased.

[1] National Research Council, 1991, pp. 49-50.

[2] In other words, cyber-crime consists of unauthorised acts leading to the interruption, interception, modification or fabrication of information flows. See Stallings, William: *Data and Computer Communications*, 5th edition, Prentice Hall, Upper Saddle River, 1997,cited in Chandler, Jennifer, A., 2004, p. 5.

[3] Broader definitions of cyber-crime can encompass offences related to the content of information communicated through information networks, as in Council of Europe's Cyber-crime Convention. Such an extension is not useful for the purpose of this study, which focuses on the vulnerability of information systems and networks.

*Attack tools have become more sophisticated*

The tools of cyber-crime are increasingly sophisticated, effective, and therefore difficult to neutralise for response teams.

The most serious attacks use automated tools: in a very short time frame, these are able to scan the internet for vulnerable systems while at the same time exploiting the vulnerabilities that they find, to initiate attack cycles and to coordinate attacks from multiple locations.[4] Using such features, **the Code Red and Nimda viruses propagated to a point of global saturation in less than 18 hours**. Code Red reportedly reached a spreading rate of more than 50 000 computers per hour.[5] Tools are also rapidly upgraded, or partly modified. Some have a dynamic behaviour; in other words, their characteristics can change – either randomly, or in a predefined manner, or following instructions.

Modern attack tools are more commonly conceived to operate from multiple platforms. Recent years have witnessed the fast development of distributed denial of service (DDOS) attacks, where a huge number of intermediate systems are compromised, and launch converging attacks towards one or several final target systems, with the aim of forbidding access to their legitimate users. In the 2004 CSI/FBI Computer Crime and Security Survey, DDOS attacks are by far the most costly type of crime, with 18 percent of total reported loss.[6] The survey also tends to indicate that DDOS attacks are receding from their peak in 2003, but fluctuations in the survey's pool of respondents make year-over-year comparisons very difficult (see also box 1 below).

Attack tools also increasingly have anti-forensic features, making it more difficult and time-consuming to ascertain whether a system is affected, to analyse the problem and to find its roots. A Trojan horse, for instance, can remain inactive for some time before starting to secretly communicate sensitive information to the outside, to take control of a computer or to prepare the ground for future attacks. A crucial challenge for responders is to determine quickly if attacks originating from different locations or occurring at different times are indeed independent, or if they are parts of a larger plan.

*New technologies have brought new vulnerabilities*

[4] CERT/CC: *Overview of Attack Trends,* 2002, p. 1.

[5] Statement by D. G. Wolf, director of information assurance, NSA, statement before Congress, Hearing on Cybersecurity – "Getting it right". July 22, 2003.

[6] CSI/FBI: *2004 Computer Crime and Security Survey*, p. 10.

Information and communication have experienced tremendous technological change in the past decades. However, **security considerations have been largely overlooked in the early phases of development of technologies and products**. In particular, the shift from proprietary hardware to standardised and less expensive operating systems and security products, with commonly known vulnerabilities, has dramatically increased the number of systems subject to attack. According to the CERT/CC, which collects cyber-crime statistics in the United States **since 1988, the number of detected computer programme vulnerabilities has increased four-fold between 2000 and 2002**, before slightly receding in 2003[7]. Search for vulnerabilities is increasingly automatised, and new classes of vulnerabilities appear every year.

Admittedly, the industry itself has started to address many security concerns. Soon after a vulnerability is identified, software producers often develop a corrective "patch", which they make available free of charge. It has been estimated that applying software patches to computers could protect information systems from about 95 percent of all intrusions.[8] In addition, security solutions such as firewalls and anti-virus softwares are now almost systematically adopted in OECD countries. A recent survey among US-based firms has found a dramatic increase in the use of encrypted login and files, from about 10 percent in 2002 to 58 and 69 percent, respectively, in 2003.[9]

However, a number of factors are blunting the effectiveness of such responses.

Patch application is still far from being immediate and universal. In the United States, the CERT/CC receives incident reports related to vulnerabilities one year after the corresponding patches have been made available. The so-called "time to patch" – the period during which available patches are believed to provide effective protection – is also becoming ever smaller, and administrators find it difficult to keep up to date with corrective patches. **Worryingly, the time lag between the moment a vulnerability is announced (and a patch is made available) and the moment hackers start to exploit it is also shrinking.** For the worm Witty, for instance, that delay was reduced to just one day.[10]

[7] The number of detected vulnerabilities has continued to decrease in the first half of 2004, according to the CERT/CC. This could be the result of more systematic efforts to track software vulnerabilities in recent years. However, according to a major Internet security firm, vulnerabilities are at the same time becoming more severe and easier to exploit (Symantec, *Internet Security Threat Report*).

[8] General Accounting Office, 2004c, p. 7.

[9] Computer Security Institute/ Federal Bureau of Information, 2004.

[10] Ibid.

User facility of IT protection tools is also questionable. A survey carried out by the National Cyber Security Alliance (NCSA) and America Online between September and October 2004, one of the most comprehensive in-home surveys ever conducted in this field, found that the majority of users participating in the survey lacked basic protection against viruses, spyware, hackers, and other online threats.[11] For instance, 67 percent of respondents did not have any firewall protection. The same share did not have current anti-virus software (updated within last week), although 63 percent had been the past victim of a virus infection and 19 percent had at least one virus infection currently on their home machine. Furthermore, knowledge levels were low about the different types of protection. 58 percent of respondents did not understand the difference between a firewall and anti-virus software very well or at all, and 53 percent did not understand what a firewall is and how to use it. At the same time, 84 percent of respondents reported to keep sensitive information (health or financial records, etc) on their home computers, and 72 percent said they used their home computer for sensitive online transactions like banking.

What makes protection more complex is also that the security of a system does not boil down to that of its elements. As emphasised in a recent report of the United States National Research Council, "the precise software configuration of any operational system (including applications, device drivers, and system patches) has almost certainly not been tested for security – there are simply too many possible configurations to test more than a small fraction explicitly. As new applications and device drivers are installed over time, an operational system is more likely to exhibit additional vulnerabilities that an attacker might exploit".[12] In practice, it is estimated that protection is often used in an inadequate manner. In many cases, for instance, firewalls have been installed in a configuration that makes them ineffective. Efforts to map potential system vulnerabilities *ex post* are costly, time-consuming and possibly superfluous in a constantly evolving threat environment.

According to the US CERT, technologies are increasingly designed to bypass typical firewall configurations even when protocols are marketed as "firewall friendly" (e.g. the Internet Printing Protocol and the WEB-based Distributed Authoring and Versioning).[13] In addition, some aspects of "mobile-code" (ActiveX controls, Java, and Javascript) make it difficult for vulnerable systems to be protected and malicious code to be discovered.

[11] All figures from the AOL/NCSA Online Safety Study.

[12] National Research Council, 2002.

[13] CERT/CC: *Overview of Attacks Trends*, available at www.cert.org.

The increased use of multimedia, high-technology mobile products (PDAs, portable PCs, mobile phones) with increasing storage capacities may jeopardise sensitive information. Not only are these devices exposed to theft, but they normally do not have the same level of protection (firewalls, antivirus programmes, etc.) as fixed equipment, and are to an increasing extent directly connected to enterprise networks. Likewise, the emerging trend of tele-working[14] is a source of concern, since home PCs often have a lower level of security than those in the enterprise network. If the home user is connected to the Internet, a backdoor could be created to the entire enterprise system. Broadband infrastructure development, when it is not accompanied by enhanced security provisions, also seems to facilitate the development of malicious activity. A recent OECD report noted, for instance, that Korea "has put a major effort into the development of consumer broadband infrastructure in recent years, with considerable success", but also "figures among the countries with the highest occurrence of attacks per 10 000 Internet users".[15]

Finally, wireless technologies could make matters more difficult. The Norwegian survey on cyber-crime shows that only 30 percent of wireless networks are protected by encryption technology.[16] In mid-June 2004, the world's first wireless Bluetooth worm, EPOC Cabir, was detected. The worm was relatively harmless, apart from shortening the battery life of the device by constantly scanning for other Bluetooth-enabled devices, but in this way, even printers could be attacked if located within range (and Bluetooth-enabled).[17] Security analysts are, however, mixed about future prospects of mobile viruses, and EPOC Cabir might remain a singular event as was the case with a PDA virus detected four years ago.[18]

*Critical infrastructures have become dependent on the security of information systems and networks*

**The potential damage resulting from cyber-crime increases as systems of critical importance for society become dependent upon the functioning of information infrastructures**. Nowadays nuclear power plants, air and railway traffic, financial transactions and hospitals are managed through computers and information networks. With the implementation of modernisation and e-governance plans in public administrations, a large number of governmental services also become accessible through information

[14] According to the British National Statistics, the total number of teleworkers in the UK increased by between 65 and 70 per cent over the period 1997 to 2001.

[15] OECD International Futures Programme, 2004.

[16] *Mørketallsundersøkelsen* 2003.

[17] Symantec security response threat evaluation.

[18] BBC News article, 16 June 2004, http://news.bbc.co.uk/1/hi/technology/3809855.stm, accessed 12 August 2004.

networks. Computers or computing devices are also increasingly embedded in other appliances, and then networked.[19] Information systems have become the cornerstone of critical infrastructures.

Although no serious incident affecting critical infrastructures has yet been reported, some events raise concern about the possible society-wide impacts of cyber-attacks. **In January 2003, Slammer, the fastest spreading worm to date, infected the business computer network of the Davis-Besse nuclear power plant (Ohio), and disabled one of the plant's safety monitoring systems for nearly five hours**.[20] The worm also nearly blacked out a 911 calling centre in Seattle (Washington);[21] led to the shutdown of Internet service providers in South Korea; disrupted Continental's plane schedules as it hit the airline's corporate networks and disabled the ticketing system;[22] halted Bank of America's ATM transactions after having gained access to the machines that control the ATM network in Charlotte, North Carolina; and found its way into the internal network at J.P. Morgan Chase & Co., in New York, where it caused major network slowdowns and nearly halted e-mail traffic.[23]

*The scope of cyber-crime has considerably increased*

There are large uncertainties regarding the overall scope and economic impact of cyber-crime.

To begin with, information is scarce. **Surveys in various countries consistently indicate that only a small fraction of organisations which have suffered a cyber-attack report it to law enforcement authorities or governmental statistics offices**.[24] One reason for under-reporting is that many attacks are simply not detected. In a recent large-scale survey in the United States, one-third of the respondents were not aware of the number of incidents having affected their computer system in the last 12 months.[25] In addition, the attacked individual or organisation may not know about reporting possibilities, or may consider that the incident is not significant enough. Finally, revealing information might considerably increase the cost of the attack for the target organisation, by tarnishing its reputation and image,

[19] National Research Council, 2001.

[20] Poulsen, Kevin, 2003.

[21] O'Harrow, Robert Jr. and Ariana Eunjung Cha, 2003.

[22] Chen, Anne, 2004.

[23] Fisher, Dennis, 2003.

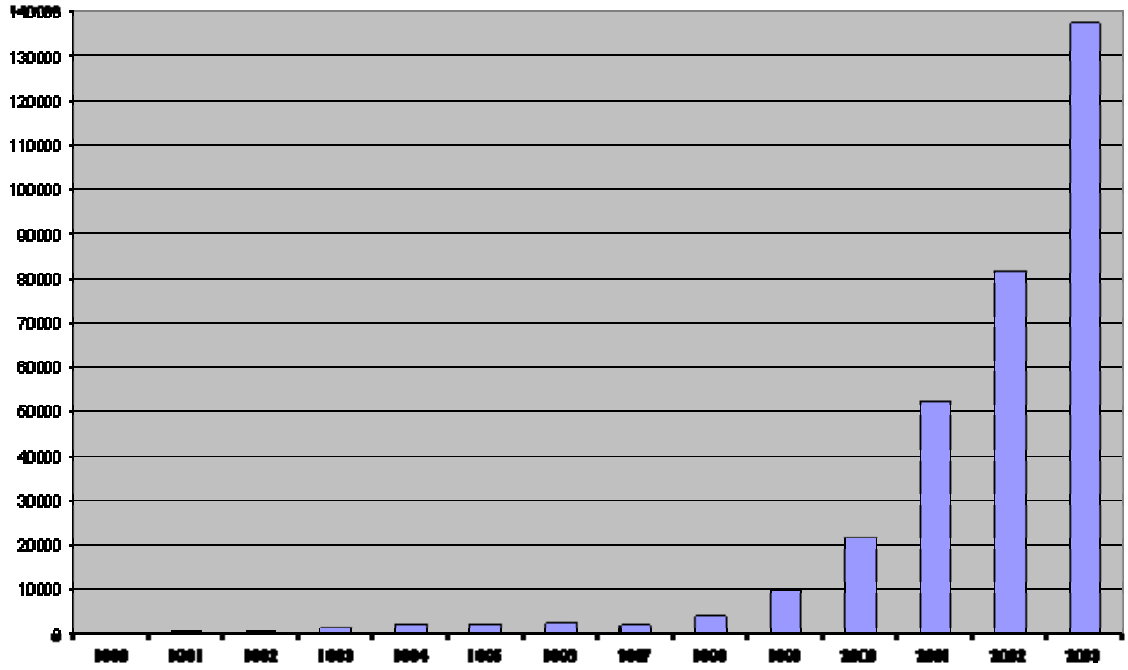
[24] See, for instance, the Norwegian Industry Security Council, 2003; the Australian Computer Crime and Security Survey 2004, published by AUSCERT; and the pilot test of a computer security survey in the United States by the Census Bureau.

[25] Computer Security Institute/ Federal Bureau of Information, 2004.

deteriorating its valuation on financial markets, or triggering litigation and liability procedures. In 1995, after Citibank declared that it had experienced an information security incident, its competitors immediately used this information to lobby some of its major clients. Some estimate the resulting loss in revenue for the bank to about USD 100 million.[26] Strong incentives not to disclose information are one of the core issues information security policy has to deal with.

The phenomenon is also difficult to measure. For instance, the CERT/CC collects the number of reported incidents in the United States, regardless of the severity of an incident and of the number of computers that it affected, as a simple indicator of the scope of cyber-attacks. The data indicates a continuous rise in the number of incidents since 1990, including six-fold increase in between 2000 and 2003 (see figure 1). However, at a time when an automated attack can be directed towards huge numbers of computers and systems through the Internet, this information loses much of its pertinence.[27]

Figure 1 – Incidents reported to CERT/CC, 1990-2003 [28]




[26] See Hoo Soo, K.J., 2000, p.32.

[27] For this reason, the CERT/CC has decided to stop publishing statistics on the number of reported accidents after 2003. See http://www.cert.org/.

[28] Source: CERT/CC, www.cert.org/stats/cert_stats.html, accessed 16 September 2004.

Likewise, various estimates of the costs of cyber-crime are available, but their results are widely different and their credibility is affected by serious methodological and practical shortcomings (see box 1).

Box 1 – Evaluating the costs of cyber-crime

Evaluating the costs of cyber-crime poses a number of methodological challenges. How to quantify the loss of a sensitive information asset, knowing that its eventual cost for the firm will depend on who holds it, at what time, and what use will be made of it? How to measure cascading effects, such as the repercussions of a system's disruption on other linked systems? How to account for indirect costs such as security expenses (e.g. the overheads costs of an incident response team)? There is not a standard, widely accepted method for dealing with these questions.[29]

Because of the scarcity of information and the lack of a consistent cost assessment method, estimates of the economic impact of cyber-crime are commonly based on surveys among organisations. For instance, a global survey was conducted in 2003 by PriceWaterhouseCoopers among 1000 companies in 50 countries, and found that their average loss due to cyber-crime amounted to USD 0.8 million in the two previous years. The US-based Computer Security Institute runs an annual survey with the assistance of the FBI, and finds results in the same order of magnitude (USD 0.5 million of average loss in 2003, after 0.8 million in 2002)[30]. However, such results cannot be interpreted as accurate measures of the costs of cyber-crime even among participating organisations, simply because the lack of a consistent method for quantifying costs also applies to the survey respondents. Indeed, about two-thirds of the participants to the first survey and half of the participants to the second were unwilling or unable to quantify their losses. In addition, as the survey samples do not aim at being representative, the results cannot be rigorously extrapolated to the national or global level. In the case of the US survey, the survey sample changes every year, which makes it difficult to analyse evolutions from one year to the other.

Some econometric studies have adopted a different approach and analysed how financial markets evaluate the costs of a cyber-attack for the targeted corporation. Several studies have found that immediately after the announcement that a firm has experienced a cyber-attack, its stock prices fall substantially (on average by about 2%) relative to the market.[31] But it is not yet clear whether these price changes are simply short-term fluctuations due to the market's reaction, or if they are persistent.

The most general cost assessments are produced by the information security industry, based on extrapolations from surveys – although the precise methodology of these assessments is usually not made public, and therefore cannot be

[29] For a discussion, see Soo Hoo (2000), op. cit., chapter 3.

[30] Available at http://www.gocsi.com/.

[31] Some studies find large differences in market reactions according to the firm's dependence on the Internet for conducting business and to the severity of the attack. This literature is reviewed in: Congressional Research Service, *The Economic Impact of Cyber Attacks*.

objectively evaluated. It has to be noted that the firms producing these estimates are vendors of security products and services. The US-based firm Computer Economics publishes an annual figure for the "worldwide financial impact of virus attacks", which surged from USD 2 billion in 1996 to USD 17 billion in 2000, and fell back to between USD 11 billion and USD 13 billion in subsequent years.[32] The estimates compiled by UK-based company Mi2g are probably the broadest in terms of scope, since they cover "economic damage from hacking, phishing, viruses, worms and spam as helpdesk support costs, overtime payments, contingency outsourcing, loss of business, bandwidth clogging, productivity erosion, management time reallocation, cost of recovery, software upgrades, Intellectual Property Rights (IPR) violations, customer and supplier liabilities and share price decline where applicable". The results are astronomic: USD 225 to 275 billion in 2003, and USD 186 to 228 billion between January and March 2004.[33]

All in all, a range of evaluations are available which largely differ in their approach, scope, methodology, and, not surprisingly, in their results. For instance, the cost estimates of the 2003 computer worm SoBig (reported in the media) went from USD 1 billion to USD 31 billion.[34] Based on available information, even a qualitative assessment of the situation is somewhat uncertain: as observed by the US Congressional Research Service, "between 1997 and 2003, attack or crime costs either doubled (according to CSI/FBI data), quadrupled (according to CEI), or went up a hundredfold (Mi2g)".[35] Depending on the source, the worst year in terms of loss has been 2000 (CEI), 2002 (CSI/FBI), or 2004 (Mi2g).[36]

In summary, it is unquestionable that cyber-crime has continuously developed and imposed increasing costs on organisations and individuals throughout the 1990s (and particularly in recent years), and that these costs have added up to tens of billions of US dollars a year in recent years. However, more precise assessments of the scope and impact of cyber-security face two major obstacles: lack of data due to inadequate information sharing, and measurement issues inherent to information security.

[32] http://www.computereconomics.com/

[33] http://www.mi2g.com/cgi/mi2g/press/faq.pdf, last update 17 March 2004, accessed on 26 August 2004.

[34] Congressional Research Service, 2004, p. 12.

[35] Ibid., p. 11.

[36] Ibid.; pp. 9-12.

## Cyber-security policy in selected OECD countries

Determining the role governments have to play in order to achieve an acceptable level of security in information systems and networks is not a straightforward task. To date, the development of information technology and networks (in particular the Internet) has been essentially driven by market forces. While a number of factors make a strong case for governmental action in the area of information security, there are also important limits to what governments can achieve. Governmental policies therefore have to be carefully crafted, and take advantage of the substantial body of national and international initiatives undertaken in the past years.

*The case for and limits of governmental intervention in the field of cyber-security*

Improving cyber-security can come at a cost for individuals and organisations: it mobilises resources in bandwidth, computing power, memory, money and time (for personnel training, management of security, etc.), and usually leads to reduced functionality of the system (restricted access for some system users, heavier procedures, etc.).

At the same time, the benefits of security expenditure are smaller for the organisation or individual who engages that expenditure than for society as a whole – in other words there are positive externalities to information security. There are three channels through which security-enhancing investments engaged by one participant in a network benefit others: first, by making attacks more difficult, and hence reducing risks over the network (particularly for attacks using intermediate target systems); second, by making the network more reliable and thereby supporting its development (e.g. fostering e-commerce); third, by ensuring that the supply of goods and services produced by an organisation will not be disrupted following an attack of its information systems.[37] Conversely, a participant's lack of consideration for security generates costs for other participants.

Under such conditions, economic theory concludes that individuals and organisations invest less, on average, in the security of their information systems than what would be optimal from a collective standpoint. Free riders take advantage of the efforts engaged by others, and inadequate overall security limits the development of the network (e.g. communication and commerce on the Internet).

[37] The latter type of externalities can be substantial, for instance in the case of critical infrastructures where disruptions related to computer problems can have considerable costs for large parts of the society. They can be partly internalised through liability procedures related to business interruption.

Incentives to enhance security seem also inadequate on the software and hardware supply side, in a market which is primarily focused on functionality. So far, the prevailing practice has often been to commercialise products first and to test their security aspects only afterwards, and to distribute patches to users at minimal costs for the producer.

The argument of externalities also applies to information-sharing. As stated earlier in the paper, the costs of disclosing information related to an attack are private, while its benefits largely accrue to society, be they related to better assessment of cyber-threats or to improved capacities to mitigate an ongoing attack.

It is the role of public policy to correct such market failures. The short history of governmental policy measures in the area of cyber-security shows, however, that such measures are subject to a series of constraints.

First, reliable information for designing and calibrating public policy is very limited. The number of virus infections, security breaches and other attacks and the damage that they cause are not well known. Because of the lack of information, traditional decision support tools such as cost-benefit analyses are difficult to apply to the field of cyber-security.[38]

Second, the improvement of security needs to be combined with the promotion of basic rights such as the right to privacy, freedom of expression and freedom of communication. For instance, disclosure of information to law enforcement authorities can be problematic, even when that information is not strictly confidential.[39] The law has to determine the exact limits of what is achievable for public authorities in the framework of their policies in support of cyber-security.

Third, people and organisations can be reluctant to adopt security-enhancing measures which significantly reduce the functionality of information systems. Attempts to improve the protection of an information system can make the system more cumbersome to access, less interoperable with other systems, or less user-friendly. For instance, the use of multiple passwords may improve the security level, but it increases the burden of the user.[40] The failure of the US government's Orange Book is a good illustration of this. The

[38] Computer Science and Telecommunications Board, National Research Council, 2003, p. 64.

[39] ISAC Council Working Paper, 2004a, p. 2.

[40] Computer Science and Telecommunications Board, National Research Council, 2002, pp. 11-12.

government demanded secure systems from the industry, but federal agencies refused to buy them as they were slower and less functional than other available, less secure systems.[41]

Fourth, as cyber-security is by nature a global public good, and as information systems interdependencies spread well beyond national borders, cyber-security policies can only be effective if they are internationally co-ordinated.

*International initiatives in the area of cyber-crime and cyber-security*

International fora have played a leading role in exploring consistent policy responses to the challenges of cyber-security in recent years. Three initiatives have been of particular importance in establishing a framework for national cyber-security policies: the Council of Europe's Cyber-crime Convention, G8 cooperation in the fields of critical information infrastructure protection and high-tech crime, and the OECD's Guidelines for the Security of Information Systems and Networks.

The Council of Europe's Convention lays the foundations for a harmonised criminal policy against cyber-crime, by creating obligations for its signatory parties both in terms of national legislation[42] and international co-operation[43]. The objective of the Convention is to facilitate the investigation, punishment and deterrence of criminal offences committed through information systems and networks. It is therefore outside of the scope of this paper, i.e. the protection of information systems from a vulnerability reduction standpoint. Still, it needs to be noted that the Convention is the first international treaty on cyber-crime, that it has been elaborated by a large group of countries (the 45 members of the Council as well as Canada, Japan, South Africa and the United States) and opened to signatures in Budapest on 23 November 2001. The Convention has since been signed by 32 countries and ratified by 6, and has entered into force on 1 July 2004.

In 2003, France and Germany co-sponsored a G8 meeting on the protection of critical information infrastructure. The meeting was the first of its kind organised at the international level and resulted in eleven general principles addressing the issues of: cyber-crime prevention, reporting and information-sharing on incidents and vulnerabilities; creation of national and international networks between public and

[41] Ibid., p. 9.

[42] These include the definition of offences; establishment of appropriate liabilities and sanctions; provisions for effective investigation; rules regarding the preservation, search and disclosure of stored computer data; and safeguards regarding the protection of human rights and liberties,

[43] Notably principles relating to extradition, mutual assistance, spontaneous information, requests for assistance, confidentiality and investigative powers.

private stakeholders; reduction of infrastructure vulnerability through the identification of interdependencies and improvement of response capacities; and creation of an adequate legal framework.

The G8 countries undertook to cooperate in the area of high-tech crime through a 24 hours/7 days information network. The network, established between 1998 and 2000, has since been opened to other countries, and currently has about 25 members. In addition, the G8 subgroup on High-Tech Crime has endorsed the Interpol information network, the *National Central Reference Points*, which lists responsible experts within more than 85 countries (still in expansion). This network should also be operable 24/7.

The OECD Guidelines for the Security of Information Systems and Networks were adopted by the Organisation's Council on 25 July 2002, as a revision of the 1992 OECD Guidelines for the Security of Information. The Guidelines are a set of nine principles to be followed by all participants to information systems and networks, according to their relative roles and responsibilities:[44]

- Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

- Responsibility: All participants are responsible for the security of information systems and networks.

- Response: Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

- Ethics: Participants should respect the legitimate interests of others.

- Democracy: The security of information systems and networks should be compatible with essential values of a democratic society.

- Risk assessment: Participants should conduct risk assessments.

- Security design and implementation: Participants should incorporate security as an essential element of information systems and networks.

- Security management: Participants should adopt a comprehensive approach to security management.

[44] *OECD Guidelines for the Security of Information Systems and Networks*, 2002.

- Reassessment: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

The major aim of the Guidelines is to promote a culture of security among all participants, and to encourage co-operation and information-sharing between them. Their focus, therefore, is not specifically on protection and vulnerability reduction policies, but more broadly on "the adoption of new ways of thinking and behaving when using and interacting within information systems and networks". A follow-up project on the implementation of the Guidelines by Member Countries is currently underway at the OECD.

*Five broad areas of governmental action have emerged*

All OECD countries have engaged actions to address the challenges of cyber-security in recent years, and many are considering taking additional measures in a not-too-distant future. Five broad areas of action can be identified in a myriad of recent policy measures: raising awareness and improving information-sharing; enhancing vulnerability detection and response; promoting more secure products and services; securing governmental and critical information systems and networks; and developing an adequate legal framework.

It is crucial, however, to note that defining and implementing a consistent and comprehensive strategy to enhance cyber-security is an ongoing task in most if not all countries. Considering the rapidly evolving threat environment, emerging public policies in the area of information security need to be kept under constant institutional scrutiny, and to be re-oriented, improved or rationalised if need be, before they produce undesirable effects.[45]

(1) Raising awareness and improving information-sharing

Governments need to inform individuals and organisations about the risks related to cyber-crime, the potential consequences of inadequate security for oneself and for others, and available solutions.

Most OECD countries have launched awareness-raising campaigns in recent years, through conferences, publications, dedicated websites, etc. Communication has targeted the general public, or in some cases, more restricted audiences such as businesses, small and medium enterprises, new users, and young people. In Germany, 1 million CD-ROMs have been distributed, and, in partnership with a major computer producing company, background information has been preinstalled on new computers.

[45] The US General Accounting Office is a good example of such a national monitoring unit.

Initiatives have also been taken by private actors, with or without the support of governments, in order to facilitate and encourage the exchange of information. One model is that of the *Information Sharing and Analysis Centers* (ISAC), which are industry-specific networks for disseminating up-to-date information, sharing experiences, and promoting industry-government co-operation based on trust in the field of cyber-security. [46]

ISACs are a common form of industry organisation in the United States, in particular for critical infrastructure sectors (see also section (4) below). In April 2004, 15 critical infrastructure ISACs were identified in the country, including in financial services (the first of all ISACs, established in 1999), telecommunications and electric power generation. Most of them address cyber-threats and are supported by governmental funds.[47]

In the United Kingdom, two alternative forms of information-sharing structures are supported by the government (specifically by the National Infrastructure Security Co-ordination Centre).[48] *Information Exchanges* are regular confidential industry forums with representatives from about 50 private sector companies, covering finance, telecommunications and sectors dealing with Supervisory Control and Data Acquisition (SCADA) systems. *Warning, Advice and Reporting Points* are small, inter-linked, community-based information-sharing cells, conceived as a cost-effective alternative to ISACs.

In 2004, the European Union created a similar body at the regional level, called the *European Network and Security Agency* (ENISA). ENISA's mission is to foster network and information security among Member States and to serve as a centre of expertise for Member States and EU institutions.

(2) Enhancing vulnerability detection and response

As showed earlier, effective vulnerability detection, vulnerability reduction and response to attacks constitutes one of the crucial challenges of cyber-security.

*Computer Emergency Response Teams* have been created to meet this need. The main responsibility of CERTs is to detect and inform about vulnerabilities; to make patches available to organisations and to the general public; to provide technical assistance in dealing with computer incidents; and to co-ordinate response in emergencies. CERTs can operate on a nation-wide basis, inside the governmental sector, or

[46] ISAC Council, 2004b.

[47] General Accounting Office, 2004b, pp. 18-22.

[48] Wenger, Andreas and Jan Metzger (eds.), 2004, p. 193.

within a specific industry. They form an international cross-sectoral network of information exchange[49] through the *Forum of Incident Response and Security Teams* (FIRST), the leading incident management organisation at the international level, created in 1992.[50] FIRST nowadays gathers more than 100 governmental, military and private CERTs, with representation from most world regions. Its action has prompted the further development of CERTs at the national level.

Governments have a role to play in initiating, supporting or operating such structures – in fact, the most wide-reaching CERTs are based on public-private partnerships. The InfoSurance Foundation, a Swiss organisation and supported by leading companies and the government, is a good illustration. At its creation in 2002, InfoSurance performed an ambitious national risk analysis focusing on interdependencies of information infrastructures within and between sectors. Currently, its main tasks consist in raising awareness of information assurance, developing prevention measures and establishing networks of cooperation.[51]

In the United States, the US-CERT was launched in 2003 with the ambition of networking private cyber-security vendors, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local governments, and domestic and international organisations, to "coordinate national and international efforts to address key cyber-security issues".[52]

(3) Promoting more secure products and services

Governments have important tools to encourage the development of more secure IT-related products and services, in particular security standards and certification procedures, their own procurement policies, and support to research and development.

Several OECD countries have developed or promoted standards and certification mechanisms related to the security of softwares or the management of information safety. At the international level, efforts to establish standards have been co-ordinated notably by the *International Organization for Standardisation* (ISO), and led to the development of two widely accepted norms: ISO/IEC 15408 for security assessment of IT-products, and ISO/IEC 17799 for security management inside organisations. ISO/IEC 15408

[49] Glaessner, Thomas; Kellermann, Tom and McNevin, Valerie, 2003, p. 73.

[50] Information from FIRST's website, available at http://www.first.org/about/first-description.html, accessed 13 August 2004.

[51] Wenger, Andreas and Jan Metzger (eds.), 2004, pp. 179-180.

[52] http://www.us-cert.gov/.

establishes "evaluation criteria for information technology security" (also known as "common criteria") for defining, assessing and comparing the security performances of IT products. ISO 17799 is a "code of practice for information security management", which defines ten areas of information security management in an organisation (from business continuity planning to security policy) and offers guidelines in each area. These standards are now directly used by some countries, and also by the emerging cyber-risk insurance business.[53]

Governments can also support the emergence of secure industry products through public procurement, provided decisions are taken in close co-operation with the end users (i.e. public administrations and agencies) and the manufacturers. As demonstrated by the pitfalls of the US government Orange Book initiative, it is crucial to precisely assess the needs of end-users not only in terms of security, but also of functionality. A possible model could be that of public procurement policies in domains such as safety-critical softwares (software on which human lives depend, used in aviation, nuclear reactors etc), which already have a strong security focus. The UK Ministry of Defence standard 00-55, for instance, "refers to a number of procedures, techniques, practices and tools which when followed or used correctly will reduce but not necessarily eliminate the probability that the software will contain errors."[54]

Public Key Infrastructure (PKI) for electronic signatures provides an example of governmental support in favour of an emerging technology, in a related (but distinct) field. In 1999, a European Union directive on electronic signatures was adopted to create a common market for product vendors and service providers and promote general legal acceptance of electronic signatures. Several countries (EU and non-EU) have since established dedicated bodies to coordinate and monitor the implementation of this infrastructure of secure electronic commerce and electronic messaging or other government activity requiring public key cryptography. In addition, research programmes have been launched to create interoperable standards (numerous programmes at the EU-level only: pki Challenge, ESTIO, TIE). So far, however, market uptake has been low due to complex requirements, low user benefits of obtaining a certificate, lacking common software, as well as data protection issues (how combine the use of pseudonyms with electronic authentication).[55]

Finally, governments can provide support for security-enhancing education, research and development, notably by prioritising IT-security in their own research agendas, or through public-private partnerships.

[53] Glaessner, Thomas; Kellermann, Tom and McNevin, Valerie, 2003, :*op. cit*., p. 57

[54] UK MoD, DEF STAN 00-55, Part I: Requirements, numbered heading 2.

[55] Jos Dumortier et al., 2003, p. 138.

For instance, United States' National Strategy to Secure Cyber-Space comprises the elaboration of a federal government IT security research agenda covering issues such as intrusion detection, Internet infrastructure security, application security, Denial of Service, and high-assurance systems. In addition, the plan charges the Department of Homeland Security with reviewing, and if necessary developing, mechanisms of co-ordination for research and development between academia, industry and government. Recently, the DHS and the National Science Foundation have also agreed to join efforts to increase the number of skilled students in the fields of information assurance and computer security[56]. In Japan, the government provides training and a certification programme for IT security professionals[57].

(4) Securing governmental and critical information systems

Governments have responsibilities as owners and operators of information systems. In recent years, the context of governmental IT security has considerably evolved with measures to avoid the Y2K problem, the aftermath of September 11, the implementation of e-governance programmes and the challenges of cyber-crime. Guidelines for governmental services have been elaborated, and teams, agencies and inter-ministerial committees dedicated to cyber-security have been created. The looming organisation of governmental IT security differs widely from country to country, but with some common features.

There is usually one (or several) *Computer Emergency Response Team(s)* dealing with issues of vulnerability detection and reduction, warnings, and incident response for governmental information systems. The (principal) governmental CERT is in most cases related to or integrated in a governmental service with a broader mandate, including for instance the elaboration of IT security guidelines and recommendations for agencies and ministerial departments; technical assistance to agencies and departments and training services for civil servants; development of standards and common criteria for certification; co-operation with the private sector.[58]

The degree of monitoring of information security policies implemented by agencies and departments is variable: some countries have a totally centralised approach as far as security is concerned; others have elaborated common guidelines, and left it to agencies' and ministries' responsibility to conform to those; in others, finally, ministerial departments have full responsibility for the security of their information

[56] http://www.us-cert.gov/press_room/schlrshp_srvce.html, consulted on 13 September 2004.

[57] OECD, 2004.

[58] These missions can also be shared between two or more services, as for instance in the United Kingdom (see same section, below).

systems. When responsibilities for policy implementation are decentralised, a mandate is sometimes given to a governmental service to verify the actual security of governmental sites and systems.

Efforts are also undertaken to co-ordinate decentralised approaches, but they can face obstacles, as demonstrated by current efforts to improve patch management inside the US federal government. In February 2003, the FedCIRC (Federal Computer Incident Response Center, now part of the US-CERT) initiated a Patch Authentication and Dissemination Capability (PADC) to provide users with a method of obtaining information on security patches relevant to their enterprise and access to patches that had been tested in a laboratory environment. This service was free for federal civil agencies. Subscribers could receive notification and download profile-specific patches. However, usage turned out to be very low, and the service was ended in February 2004. Agency officials claimed that not enough licenses were issued; that the service did not support all platforms and the level of services was low. [59]

Governments can also take an active part in the management of cyber-security in critical infrastructures, due (as noted above) to the existence of strong externalities.

The German *Federal Office of Information Security*, for instance, takes care of every aspect of IT safety and technical support in both the government networks and critical infrastructures. Another example is the inter-departmental UK National Infrastructure Security Coordination Centre (NISCC), which focuses entirely on the coordination of critical IT infrastructure protection, cooperation with private infrastructure owners, the development of general risk and vulnerability analyses and IT emergency management. The UK government CERT, UNIRAS, is connected to NISCC. In the United States, the government has just launched the Protected Critical Infrastructure Information Program, which "enables members of the private sector to, for the first time, voluntarily submit confidential information regarding the nation's critical infrastructure to the Department of Homeland Security (DHS) with the assurance that the information will be protected from public disclosure". The programmeme is an attempt to resolve the possible conflict between the needs of collecting information to better protect critical infrastructure, and the costs of disclosing that information for infrastructure operators.

(5) Developing an adequate legal framework

Last but not least, the legislative apparatus can be a powerful tool for combating cyber-crime and increasing cyber-security. To this aim, most OECD governments have taken important measures in the

[59] GAO, 2004c, p. 23.

area of criminal law, more or less in line with the Council of Europe's Cyber-crime Convention. A commonplace measure has consisted in establishing legal equivalence between electronic documents and written documents, in order to provide to the former the same degree of legal protection as the latter.

Recent developments and ongoing reflections in the area of civil law might be of particular interest from a vulnerability reduction standpoint. In several countries, privacy laws have been passed to ensure that consumers' personal data held by commercial firms are adequately protected.

In the United States, the Financial Modernisation act of 1999 (also known as the Gramm-Leach-Bliley act) defines requirements for financial institutions and other firms collecting or holding consumers' personal financial information, including rules for the design, implementation and maintenance of safeguards. The Federal Trade Commission has also brought several cases in recent years against companies which allegedly deceived consumers by not taking measures to protect personal information as claimed in their privacy policies. These cases were resolved by consent agreements requiring that the respondents (commercial firms) establish a comprehensive information security programme, and submit it to an annual audit to certify that it meets certain minimum requirements.

In Europe, the European Commission has developed a legislative framework for data protection in order to co-ordinate new legal developments in the EU Member States, notably with the directives 95/46/EC on the protection of individuals with regard to the processing of personal data, and 2002/58/EC on privacy and electronic communications.

Directive 95/46/EC harmonised hitherto differing approaches to data protection among Member States of the EU. It established, in particular, principles of personal data quality (article 6); criteria for the legitimacy of data processing (article 7); categories of sensitive data which cannot be processed (article 8); notification obligations (articles 10 and 11); and rights of access (article 12). Importantly for the subject of this study, it obliges the controller[60] to implement technical and organisational measures in order to protect data from accidental or unlawful destruction, loss, alteration, disclosure or access, including during transmission over a network (article 17). A general description of those security measures, which would allow a preliminary assessment of their level of appropriateness, must be notified to the authorities (article 19). Appropriateness depends on the risks and the nature of the data, "having regard to the state of the art and the cost" of implementation of the measures. The directive also extends to international transfers of personal data, defining adequate levels of data protection in third countries.

[60] i.e. the person, natural or legal, who "determines the purposes and means of the processing of personal data".

Directive 2002/58/EC enhances data protection rules across the telecommunications sector - including telephony, e-mails, internet use and SMS messaging. It requires Internet Access Providers to ensure the security of the communications that they provide (on the same bases than the directive 95/46/EC in its article 17). Data protection no longer makes a distinction between data sent via traditional networks or data sent via the Internet. The directive also prohibits unsolicited communications, i.e. it requires companies to obtain a person's positive consent as a precondition to any other communication.

Finally, the European Commission elaborated in 2001 the Framework decision on attacks against information systems, which seeks to address cyber-crime by harmonising national legislations applicable to offences committed against a computer infrastructure. The decision provides a definition of illegal access to and illegal interaction with an information system, while restricting its scope to cases where it can be proved that the action was intentional. It covers both offences affecting Member States and offences committed from their territory. The Framework decision was adopted by the EU Council in February 2005, and Member States have to implement it by February 2007.

## The management of information security in Norway

*The policy context*

As in other OECD countries, the legislation and institutions dealing with IT-security have been dramatically evolving since the end of the 1990s. Two reports issued in 2000 have had a strong influence on recent changes: the Governmental Commission on the Vulnerable Society's report, and the Ministry of Trade and Industry's report on cyber-security. Both highlighted the emergence of cyber-security as a risk area of critical importance, and made recommendations for a strengthened policy approach to it. They led to the elaboration of a National Strategy on IT-Security, adopted in July 2003, which aimed at reducing vulnerabilities related to information systems and networks, promoting a culture of IT-security[61] and facilitating electronic commerce through a series of strategic orientations:[62]

- Adequate protection of critical IT-infrastructures
- Co-ordinated development and enforcement of IT-security regulations
- Creation of a national Information Security Coordination Council
- Use of risk and vulnerability analyses as the basis for security measures both at national and company level
- Categorisation of information and information systems with regard to their security implications
- Awareness of all participants
- Warning and advice for protection of systems, prevention of attacks and damage limitation
- Responsibility of IT-vendors and service providers for the security of their products and services, on the basis of self-regulation and if needed, governmental regulatory action
- Use of certified security components and solutions for critical IT-systems and infrastructures
- Increased R&D, higher education curricula and courses at all educational levels in IT-security

[61] In its broad-based approach for promoting a culture of security in society, the Strategy builds on the OECD Guidelines on the Security of Information Systems and Networks.

[62] Norwegian Ministry of Defence, Ministry of Trade and Industry, Ministry of Justice and the Police, 2003.

- Creation of a national infrastructure for electronic identification and electronic signatures
- Active participation in international arenas for cooperation on information security

The implementation of the Strategy and other parallel policy measures have produced an extensive body of laws and regulations directly or indirectly related to IT-security, as well as a new governmental organisation for IT-security management.[63]

The *Ministry of Justice and the Police* has overall responsibility for national security in peacetime, including a coordination role with regard to the protection of critical information networks and systems. The *Directorate for Civil Preparedness* (DSB), the technical arm of the Ministry, has an underlying department dedicated to national preparedness planning which elaborates preparedness plans and risk and vulnerability assessments.

The *Norwegian National Security Authority* (NSM) coordinates preventive IT-security measures and controls the level of security in undertakings covered by the 1998 Norwegian Act Relating to Protective Security Services. These include central and local public administration, as well as private suppliers of goods and services to the public, when the purchases concerned are "security sensitive" or classified. NSM also collects and evaluates relevant information, develops technical and administrative security measures, issues regular threat evaluations and vulnerability reports, and gives advice. NSM was established 1 January 2003, and reports to the Ministry of Defence on military issues and the Ministry of Justice on civil issues. NSM is funded and administrated by the Ministry of Defence.

NSM is hosting SERTIT, a public Certification Authority for IT Security in Norway. Its primary task is to issue Certificates and Certification Reports. SERTIT is representing Norway as a member of the international community called "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security" (CCRA).

A branch in NSM is the *Warning System for Digital Infrastructures* (VDI), a network between major private and public infrastructure operators and intelligence authorities (PPP).

[63] Only the major institutions in charge of defining and implementing the government's IT-security policy are listed here. A more complete description of governmental responsibilities, following the Project's methodological framework, is proposed in Annex 1.

Within NSM, a project "NorCERT" has been launched as an effort to explore a concept for establishing a National CERT. A principle task for "NorCERT" is to coordinate response to cyber attacks on critical infrastructure in public and private sectors in Norway.

The *Ministry of Modernisation* co-ordinates IT-security for non-classified information and systems.[64] A *Centre for Information Assurance* (SIS) has been created as a three-year pilot project and placed under the Ministry's jurisdiction. SIS is a public-private partnership, and mainly deals with awareness-raising among public and private actors and emergency management. SIS is connected to a university sector CERT, UNINET CERT. International cooperation and the creation of networks with private actors are among its principal objectives. The main long-term objective of the SIS project is to establish a centre responsible for the national coordination of incident reporting, alerts, analysis and experience-sharing.

The *Data Inspectorate*, an independent administrative body under the Ministry of Modernisation, is in charge of enforcing legislation on personal data (in particular the Personal Data Act of 2000), which contains binding regulations regarding the security of systems (both public and private) where personal data is processed.

The *National Information Security Co-ordination Council* (KIS) was established in May 2004 to supervise the strategic orientations and overall consistency of governmental IT-security policies. The group, chaired by the new Ministry of Modernisation, consists of representatives from seven ministries, the Prime Minister's office and nine different directorates. NSM acts as the Council's secretariat. Questions addressed in the Council include IT-security and questions related to national security, national security interests and critical infrastructure. The Council shall furthermore coordinate the further evolution of the IT-security legislative framework, develop common standards and working methods for IT-security, and coordinate control activities. The group shall also discuss current issues related to risk and vulnerability and contribute to improved information activities and preparedness planning. The council is keeping track of the strategic orientations presented in the National Strategy for Information Security, ensuring that all responsible authorities participate.

[64] The Ministry of Modernisation was created on 1 October 2004, with the mandate of the former Ministry of Labour and Government Administration, and in addition, responsibility for the national policy for development and coordination of the use of information technology, which was previously held by the Ministry of Trade and Industry. The Ministry changed name 1 January 2006 and is now called the Ministry of Government Administration and Reform.

**Conclusion and proposal regarding the second phase of the Project**

While the precise magnitude of cyber-crime is very difficult to evaluate, there is little doubt that cyber-security has become, in only a few years, a crucial field of risk and security management in OECD countries. Because of the reliance of most critical infrastructures on information systems and networks, and because of ever-growing connectedness, breaches in information security can nowadays lead to catastrophic social and economic consequences, as occasionally demonstrated by accidents and disruptions throughout the world. Understandably, information security has recently received considerable attention from policy-makers and private actors in all OECD countries. The review of international and national policy measures presented in this paper pinpoints a number of actions in the area of cyber-security which, together, can be seen as the current "cyber-security policy toolbox" of OECD governments.

As other countries, Norway has taken a number of important legislative and institutional initiatives to enhance information security in recent years. With the National Strategy for Information Security, Norway's government has adopted an approach to IT-security which, if ambitious, is also gradual and adaptive. Most new structures are first launched as pilot projects, tested and made permanent only thereafter. A general reappraisal and renewal of the National Strategy is envisioned for 2006, on the basis of experience gained and additional analyses, under the aegis of the KIS. As explained earlier, this seems to be a wise choice considering the speed of change in the area.

The tool for self-assessment and review of policies proposed hereafter is meant as a contribution to the ongoing reflection of the Norwegian government regarding its approach to information security. It comes in three parts.

Annex 1 identifies the main actors of information-security management in Norway (and, when possible, their specific roles) according to methodology of the Project ("functional layers" column), and at a more refined level, according to the elements of the "cyber-security policy toolbox" ("actions" column).

Annex 2 lists the principal laws and regulations with direct or indirect connections to IT-security, and for each law, the authority in charge of supervising its implementation and enforcing it.[65]

Annex 3, finally, is a questionnaire for self-assessment based on four principles:

[65] The source of information regarding Norwegian institutions, laws and regulations is the National Strategy for Information Security.

- The questionnaire is based on the Project's methodology, scrutinizing separately each functional layer[66] with regard to coherence of organisation (definition of roles and responsibilities, communication and co-ordination between the major players, links with other pertinent layers, etc.), effectiveness in achieving objectives (adequate consideration of all tasks, use of relevant tools, etc), and openness on external sources (communication with stakeholders, international cooperation).[67]

- The questionnaire is adapted to the major orientations established by the Norwegian Strategy for Information Security. In particular, the Strategy builds a three-tier approach to the protection of information systems and networks, consisting in "defence in depth" for systems of relevance for national security, specific protection of critical infrastructure systems based on public-private co-operation, and the promotion of a culture of safety for the society at large. This structure is reflected in the self-assessment and review tool.

- In addition to investigating the allocation of roles and responsibilities, issues of coherence and effectiveness and so on, the questionnaire aims at clarifying some policy aspects mentioned in the Strategy. Consideration of the costs and benefits involved by different courses of action when allocating overall resources is an illustration of such aspects. The co-ordination of contingency and emergency planning is another example.

- Finally, the questionnaire tries to emphasise a few aspects which might be missing in the Strategy, notably the organisation of institutional mechanisms for feedback and reform.

Furthermore, Norway is currently implementing the OECD Guidelines for the Security of Information Systems and Networks. As part of this process, the OECD Secretariat has recently circulated an "OECD questionnaire on practical initiatives to promote a culture of security" among Norwegian authorities (as in other countries).[68] Although the scope of the two questionnaires is different, they have some common aspects of information security policy in their coverage. In all such cases, naturally, common answers can be used for the two questionnaires.

---

[66] This means that in practice, a specific part of the questionnaire will be developed for each layer (assessment, decision-making, etc.), and addressed to all the major actors involved in that layer. For actors intervening in more than one layer, the various parts can naturally be joined in a single document.

[67] See complete evaluation criteria in OECD IFP, "A Methodological Framework for Evaluating Risk Management Policies", mimeo, 2003.

[68] Document DSTI/CCP/REG(2004)4/FINAL, circulated between December 2004 and February 2005.

## Technical glossary

*Backdoor*: An undocumented means of bypassing the normal access control system of a computer.

*Distributed Denial Of Service (DDOS)*: DDOS attacks use multiple systems to attack one or more victim systems with the intent of denying service to legitimate users of the victim systems. The degree of automation in attack tools enables a single attacker to install their tools and control tens of thousands of compromised systems for use in attacks. Intruders often search address blocks known to contain high concentrations of vulnerable systems with high-speed connections. Cable model, DSL, and university address blocks are increasingly targeted by intruders planning to install their attack tools.

*Domain Name System*: DNS is the distributed, hierarchical global directory that translates names to numeric IP addresses on the Internet. The top two layers of the hierarchy are critical to the operation of the Internet. In the top layer are 13 root name servers. Next are the 'top-level domain' servers, which are authoritative form '.com', '.net', etc.; as well as the country code top level domains.

*Firewall*: A security system that is placed between the internet and an organisation's network, or within a network, and only passes authorised network traffic.

*Internet Protocol (IP)*: The precise way in which messages are passed through the Internet. All computers connected to the Internet use IP to communicate with each other.

*Malware*: Software with malign intent such as viruses, worms and Trojans.

*Patch*: A small change to software already distributed, usually to fix a problem in it.

*Red-teaming*: The development and application of adversary models and techniques to provide the capability of stressing information systems and technologies under a malevolent threat.

*Routers*: specialised computers that direct traffic on the Internet.

*Threat*: Adversary that is motivated to exploit a system vulnerability and capable of doing so.

*Trojan horse*: A malicious programme such as a virus or a worm, which is hidden in an innocent-looking piece of software, usually for the purpose of unauthorised collection, alteration, or destruction of information.

*Virus*: A programme which can spread across computers and networks by attaching itself to another programme and making copies of itself.

*Vulnerability*: Error or weakness in the design, implementation or operation of a programme or system.

*Worm*: a self-propagating malicious code. Unlike a virus, which requires a user to do something to continue the propagation, a worm can propagate by itself. Some worms include built-in DDOS attack payloads or web site defacement payloads. However, the biggest impact of these worms is that their propagation effectively creates a DDOS in many parts of the Internet because of the huge amounts of scan traffic generated, and they cause much collateral damage.

## Bibliography


AUSCERT (2004): *2004 Australian Computer Crime and Security Survey*, available at www.auscert.org.au/render.html?it=2001

BBC (2004): Online news article, 16 June 2004, available at http://news.bbc.co.uk/1/hi/technology/3809855.stm, accessed 12 August 2004.

Center for Strategic and International Studies (2003): *Structuring Government for Better Cyberdefense*, conference notes, Remarks of Representative Jim Turner, House Select Committee on Homeland Security, 11 June 2003, available at http://csis.org/tech/events/repturner_061103.htm

CERT/Coordination Center (2003): *Viruses and Worms: What Can We Do About Them?* Testimony before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 10 2003, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh

CERT/Coordination Center (2004): *Overview of Attack Trends*, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, available at www.cert.org/archive/pdf/attack_trends.pdf

CERT/Coordination Center (2004): *Statistics 1988-2003*, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, available at www.cert.org/stats/cert_stats.html

Chandler, Jennifer A.: "Security in Cyberspace: Combating Distributed Denial of Service Attacks", forthcoming 2004, *University o Ottawa Law and Technology Journal*, available at http://www.innovationlaw.org/lawforum/pages/chandler-final.pdf, accessed 12 August 2004.

Chen, Anne (2004): E-week news article: "Vulnerability Assessment Keeps Airline Flying", June 28, 2004, available at http://www.eweek.com/article2/0,1759,1617423,00.asp, accessed 11 August 2004.

Computer Science and Telecommunications Board, National Research Council (1991): *Computers at Risk: Safe Computing In the Information Age*, National Academy Press, Washington D.C..

Computer Science and Telecommunications Board, National Research Council (2001): *Embedded, everywhere*, National Academies Press, Washington D.C..

Computer Science and Telecommunications Board, National Research Council (2002): *Cybersecurity today and tomorrow: Pay now or pay later*, National Academies Press, Washington D.C..

Computer Science and Telecommunications Board, National Research Council (2003): *Information Infrastructure Protection and the Law: An Overview of Key Issues*, National Academies Press, Washington D.C..

Computer Security Institute/Federal Bureau of Investigation (2003): *2003 Computer Crime and Security Survey*, CSI, San Francisco

Computer Security Institute/Federal Bureau of Investigation (2004): *2004 Computer Crime and Security Survey*, CSI, San Francisco

Congressional Research Service (2004): *The Economic Impact of Cyber Attacks*, Washington D.C. 1 April 2004,.cited in GAO report 04-706: *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO, Washington D.C..

Coyne, Christopher & P. Leeson (2004): *Who Protects Cyberspace?* Global Prosperity Initiative Working Paper 37, Mercatus Center, George Mason University

Dumortier, Jos *et al.* (2003): *The Legal and Market Aspects of Electronic Signatures*, Interdisciplinary Centre for Law and Information Technology, University of Leuven.

European Information Technology Observatory (2004): *European Information Technology Observatory 2004, EITO, available at www.eito.com*

Fischer, Dennis (2003): E-week news article, "New Dangers Exposed in the Wake of Slammer", February 3, 2003, available at http://www.eweek.com/article2/0,3959,854634,00.asp, accessed 11 August 2004.

Fisk, Mike (2002): *Causes & Remedies for Social Acceptance of Network Insecurity,* contribution to the "Workshop on Economics and Information Security", University of California: Berkeley, 16-17 May 2002, available at http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/, accessed 12 August 2004.

Geer, Daniel *et al.* (2003): *Cyber*In*security: The Cost of Monopoly: How the Dominance of Microsoft's Products Poses a Risk to Security*, Computer & Communications Industry Association, available at www.ccianet.org/filings/cybersecurity/cyberinsecurity.pdf

Glaessner, Thomas; Kellermann, Tom and McNevin, Valerie (2003): *Electronic Safety and Soundness: Securing Finance in a New Age, Public Policy Issues*, World Bank Monograph, October 2003, Washington D.C..

Gulichsen, Steinar *et al* (2004): *Report: Strategier for informasjonssikkerhet – en komparativ studie av strategiarbeidet I Norge, USA, Australia og EU*; 21 January 2004, Kjeller; Norway

Hoo, Kevin J. Soo (2000): *How Much is Enough? A Risk Management Approach to Computer Security*, Working Paper, Center for International and Security Studies, Stanford University.

Hoo, Kevin J. Soo (2002): *How Much is Enough? A Risk Management Approach to Computer Security,* contribution to the "Workshop on Economics and Information Security", 16-17 May 2002, University of California at Berkeley, available at http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/, accessed 12 August 2004.

ISAC Council (2004): *Policy Framework for ISAC Community*, Working Paper, available at http://www.isaccouncil.org/pub/Policy_Framework_for_ISAC_Community_013104.pdf, accessed 12 August 2004.

ISAC Council (2004): *Vetting and Trust for Communication among ISACs and Government Entities*, White Paper, 31 January 2004, available at http://www.isaccouncil.org/pub/Vetting_and_Trust_013104.pdf, accessed 13 August 2004.

Lewis, James A. (2002): *Assessing the risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, December 2002, Washington D.C.

McAfee (2004): Press release, available at http://www.mcafeesecurity.com/us/about/press/mcafee_enterprise/2004/20040223_092029.htm , accessed 11 August 2004.

Mi2g (2004): News alert, 8 March 2004:"Economic Damage from Bagle, MyDoom & NetSky crosses $100bn: Financial motive behind the malware variants likely", available at www.mi2g.co.uk, accessed 11 August 2004.

National Cyber Security Partnership (2004): *Improving Security across the Software Development Lifecycle*, Task Force Report, April 1 2004, available at www.cyberpartnership.org/SDLCFULL.pdf

National Security Agency (2003): Statement by Daniel. G. Wolf before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science and Research and Development; Hearing on "*Cybersecurity – Getting it Right*", 22 July 2003

Norwegian Ministries of Defence; Trade and Industry; Justice and Police (2003): *e-Norge: Nasjonal strategi for informasjonssikkerhet*, June 2003, Oslo

Norwegian Ministry of Justice and the Police (2000): *Report NOU: 24, 2000 Et sårbart samfunn*, Oslo

Norwegian Ministry of Justice and the Police (2002): *White Paper No. 17 (2001-2002): Veien til et mindre sårbart samfunn*, Oslo

Norwegian Ministry of Justice and the Police (2004): *White Paper No. 39 (2003-2004): Samfunnssikkerhet og sivilt-militært arbeid*, Oslo

Norwegian Ministry of Transport and Communications (2001): *White Paper No. 47 (2000-2001): Telesikkerhet og –beredskap I et telemarket med fri konkurranse*, Oslo

Norwegian Post and Telecommunications Authority (2003): Policy document: *Sikkerhet og –beredskap i nett*, July 2003, Oslo

Norwegian Security Authority (2003): *Trusselvurdering 2003,* available at www.nsm.stat.no/dokumenter/EndeligversjonUgradertRV03.pdf

OECD International Futures Programme (2003): *A Methodological Framework for Evaluating Risk Management Policies*, working document, Paris.

OECD International Futures Programme (2004): *The Security Economy,* OECD, Paris.

OECD (2004): 'Summary of Responses to the Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks', Working Party on Information Security and Privacy, DSTI/ICCP/REG(2003)8/FINAL, June 2004, OECD, Paris.

O'Harrow, Robert Jr. and Ariana Eunjung Cha (2003): "Internet Worm Unearths New Holes: Attack Reveals Flaws in How Critical Systems Are Connected". Washington Post, 29 January 2003, available at http://www.washingtonpost.com/ac2/wp-dyn/A57550-2003Jan28, accessed 11 August 2004.

Poulsen, Kevin (2003): Security Focus news article: "Slammer worm crashed Ohio nuke plant network", 19 August 2003, available at http://www.securityfocus.com/news/6767, accessed 11 August 2004.

PriceWaterhouseCoopers (2003): *Economic Crime Survey 2003*, available at www.pwcglobal.com/extweb/ncsurvres.nsf/docid/65EC95F223DCDAD785256D4D004ECD3E, accessed 11 August 2004.

RAND Europe (2002): *Dependability Development Support Initiative: National Dependability Policy Overview,* available at http://www.ddsi.org/DDSI-F/main-fs.htm

Røstad, Lilian & Ø. Eilertsen (2004): *Mørketallsundersøkelsen 2003 – om datakriminalitet og IT-sikkerhet*, Næringslivets sikkerhetsråd, Oslo.

Schneier, Bruce (n.d.): "Risk, Complexity and Network Security", powerpoint presentation, unpublished, available at http://www.counterpane.com/presentation1.pdf accessed 10 August 2004.

Stallings, William (1997): *Data and Computer Communications*, 5th edition, Prentice Hall, Upper Saddle River, 1997,cited in Chandler, Jennifer A.: "Security in Cyberspace: Combating Distributed Denial of Service Attacks", publication forthcoming 2004 *University of Ottawa Law &Technology Journal*.

Symantec (2004): *Symantec Internet Security Threat Report: Trends for July 1, 2003-December 31, 2003*, Symantec, March 2004, available at http://ses.symantec.com/content.cfm?ArticleID=1539

The White House (2003): *The National Strategy to Secure Cyberspace*, February 2003, US government, Washington D.C.

UK Ministry of Defence: DEF STAN 00-55, Part I.

United States General Accounting Office (2002): *Critical Infrastructure Protection: Federal Efforts to Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, Report to the Committee on Governmental Affairs, U.S. Senate, GAO, July 2002, Washington D.C.

United States General Accounting Office (2004): *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, Testimony before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, GAO, Washington D.C., 30 March 2004

United States General Accounting Office (2004): *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*, Testimony before the Subcommittees on Cybersecurity, Science, and Research and Development and Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives. GAO, Washington D.C, April 2004.

United States General Accounting Office (2004): *Information Security: Continued Action Needed to Improve Software Patch Management*, Report to Congressional Requesters. GAO, Washington D.C., June 2004.

Wenger, Andreas & J. Metzger (2004): *International CIIP Handbook 2004*, Eidgenössische Technische Hochschule, Zürich, 2004.

Wolf, D.G. (2003): Statement before Congress, Hearing on Cybersecurity – getting it right, July 22, 2003.

## Annex 1: The policy context in Norway

The following annex briefly describes the layers of the Norwegian IT security management system. The description follows the project's methodology for analysing risk management systems.[69] The principal actors are indicated in bold.

| Functional layers | Actions | Authorities |
|---|---|---|
| Assessment | Product vulnerability assessment | • UNINETT CERT, TERT (Telecom CERT linked to the P&T Authority), other CERTs |
| | Sector-specific vulnerability assessment (national security, critical infrastructures) | • Ministry of Justice and the Police<br>• DSB<br>• NSM<br>• Sectoral departments (e.g. Post & Telecom Authority) |
| | Development and promotion of risk assessment tools | • Ministry of Modernisation<br>• Norwegian Industrial Safety and Security Organisation and trade organisations (categorisation of information) |
| Policy decision-making | Resource allocation (and cost-benefit considerations) | • KIS (advisory role) |
| | Strategy co-ordination and supervision | • KIS (advisory role) |
| Framework conditions | Development and use of standards and certification | • Norwegian Accreditation, NSM (SERTIT)<br>• Ministry of Modernisation (private sector and public sector procurement)<br>• Ministry of Defence |
| | Promotion of security-enhancing technologies | • Ministry of Trade and Industry<br>• Ministry of Modernisation (coordination of PKI use in the public sector, promotion of electronic signatures and PKI standards in partnership with service providers) |
| | Legal and regulatory framework | • Ministry of Justice and the Police (review, co-ordination)<br>• Data Inspectorate (protection of personal data)<br>• Regulatory authorities (each in their area of competence)<br>• Trade organisations, P&T Authority and Ministry of Modernisation (benchmarks for IT vendors and service providers) |

[69] See *A methodological framework for evaluating risk management policies*, background document , first meeting of the Steering Group of the Project, 3 November 2003.

| Functional layers | Actions | Authorities |
|---|---|---|
| Protection | Security of governmental services | • Ministry of Modernisation (governmental IT security guidelines)<br>• Data Inspectorate (secure processing of personal data) |
| | Security of critical infrastructures | • Ministry of Transport & Communications (robustness of the Internet infrastructure)<br>• Directorate of Social Services and Health (security policy for the health sector)<br>• DSB (security for civil emergency preparedness) |
| | Research and development | • Norwegian Research Council, Ministry of Modernisation, Ministry of Justice and the Police and Ministry of Defence (research programmes, public-private partnerships)<br>• DSB<br>• NSM |
| | Education | • Ministry of Education and Research |
| Information | Awareness-raising | • Ministry of Modernisation and Ministry of Transport & Communications (information activities)<br>• SIS (dissemination of information, reporting issues)<br>• Norwegian Industrial Safety and Security Organisation and trade organisations (corporate IT security guidelines)<br>• Ministry of Modernisation (international co-operation, OECD, ENISA)<br>• Ministry of Transport & Communications (ENISA)<br>• Data Inspectorate (processing of personal data) |
| | Information- sharing | • NSM / NorCERT<br>• SIS |
| | Warning | • VDI, SIS, UNINETT CERT, TERT, other CERTs |
| Rescue | Incident response assistance | • UNINETT CERT<br>• TERT (telecommunications) |
| Recovery enhancement | Contingency and business continuity plans | • DSB<br>• NSM |
| Feedback and organisational change | Feedback and learning mechanisms | • SIS (sources of incidents)<br>• OKOKRIM (investigations)<br>• KIS (organisational change) |

## Annex 2: The legal and regulatory framework

| Legislative framework | Enforcement authority |
|---|---|
| Act relating to Protective Security Services (Security Act, IT part) | Ministry of Defence / NSM |
| Telecom legislation (law on electronic communication) and regulations | Ministry of Transport & Communications / P&T Authority |
| Law on electronic signatures, regulation on providers of qualified certificates, etc | Ministry of Trade and Industry |
| Surveillance in the framework of the Personal Data Act | Data Inspectorate |
| Regulation on law of personal information, regulation on electronic communication with and within the government | Ministry of Modernisation |
| Regulation on the protection of classified government documents | Prime Minister's office |
| Laws on personal information, administrative procedures in the government, transparency of the government, several resolutions | Ministry of Justice and the Police |
| Civil defence law, resolutions of 24/3/76, 03/11/00 and other laws | Ministry of Justice and the Police / DSB |
| Law on financial surveillance authority /IT regulation | Financial surveillance authority |
| Central Bank Act | National Bank of Norway |
| Law on prosecution | Økokrim |
| Police Act (§17.a;b;c) | Police security services |
| Law on Intelligence | Military High Command / Intelligence |
| Law on Civil defence; Health, environment and security regulations | Industry security organisation |
| Law on Health personnel | Directorate of Health and Social Affairs |
| Social Security Act (§25) | Social Security Authority |

## Annex 3: Self-assessment questionnaire

The questionnaire proposed in the following pages for Norwegian public administrations to self-assess and take stock of their practices in the management of information security is organised in eight parts, one for each layer of security management:

A. Risk and vulnerability assessment, covering product vulnerability assessment, sector-specific vulnerability assessment in relation with national security and with critical infrastructures, and the development and promotion of risk assessment tools

B. Policy decision-making, covering strategy co-ordination and supervision, and resource allocation for risk management options

C. Framework conditions, covering development and use of standards and certification, the promotion of security-enhancing technologies, and the legal and regulatory framework

D. Protection, covering the security of governmental information systems and of critical infrastructures information systems, research and development and education

E. Information, covering awareness-raising, information-sharing and warning

F. Rescue

G. Recovery enhancement

H. Feedback and organisational change

In each case, the principal actors involved in information security management are listed, in accordance with the description of the management system in Annex 1. Naturally, any other relevant actors should be added to those lists.

*A. Risk and vulnerability assessment*

A.1. Product vulnerability assessment

*Principal actors: UNINETT CERT, TERT, and other CERTs.*

a. Please describe the roles and responsibilities with regard to the detection, assessment and communication of vulnerabilities in softwares and other IT products
b. What are the legal provisions and obligations relating to the assessment of vulnerabilities in IT products?
c. What are the criteria and principles used for vulnerability assessment?
d. Please provide a description of the size (budget, staff) and organisation of UNINETT CERT.
e. Which are the other principal CERTs?
f. How are these various entities (including UNINETT CERT) co-ordinated and how do they communicate?
g. What are the principal channels of information-sharing regarding product vulnerabilities with foreign and/or international entities? Which are the most important among these entities?
h. Please provide a record of product vulnerability announcements in recent years and explain the criteria for announcing a vulnerability.
i. Has the process of detection, assessment and communication of product vulnerabilities undergone important changes in recent years? If yes, please describe.
j. Do you use specific indicators or processes to evaluate the effectiveness of product vulnerability announcements? If yes, please describe.
k. What are the available mechanisms for users to report detected vulnerabilities and provide feedback? How often are they used?

A.2. Vulnerability assessment regarding national security

*Principal actors: Ministry of Justice and the police, DSB, NSM.*

a. Please describe the roles and responsibilities with regard to the identification of information systems and networks of critical importance for national security
b. How are vulnerabilities in these systems and networks assessed?
c. How are they communicated to their operators?

d. Can the operators report problems and provide feedback, and if yes, how?
e. Please describe the roles and responsibilities with regard to the evaluation of alternative possibilities for reducing these vulnerabilities, and the choice of an option
f. What are the criteria and principles used in this choice? Are costs and benefits of alternative possibilities evaluated, and if yes, how?
g. Who has responsibility for implementing vulnerability reduction measures?
h. Who has responsibility for checking that implementation is effective? When is the system tested again?
i. What are the principal channels of information-sharing with foreign and/or international entities regarding vulnerability assessment and reduction in information systems and networks of critical importance for national security? Which are the most important among these entities?

A.3. Vulnerability assessment regarding critical infrastructures

*Principal actors: Ministry of Justice and the police, DSB, NSM, sectoral supervisory authorities, and critical infrastructure operators.*

a. Please describe the roles and responsibilities with regard to the identification of critical infrastructure information systems
b. How are vulnerabilities in these systems assessed? If relevant, please make a distinction between sectoral (e.g. Post & Telecom Authority) and cross-sectoral (Ministry of Justice and the Police, DSB, NSM) departments of the government, and provide details on co-operation and communication between them.
c. How are identified vulnerabilities communicated to the operators of critical infrastructure information systems?
d. Can the operators report problems and provide feedback, and if yes, how?
e. Please describe the roles and responsibilities with regard to the evaluation of alternative possibilities for reducing these vulnerabilities, and the choice of an option
f. What are the criteria and principles used in this choice? Are costs and benefits of alternative possibilities evaluated, and if yes, how?
g. Who has responsibility for implementing vulnerability reduction measures?
h. Who has responsibility for checking that implementation is effective? When is the system tested again?

i. What are the principal channels of information-sharing with foreign and/or international entities regarding vulnerability assessment and reduction in critical infrastructure information systems? Which are the most important among these entities?

A.4. Development and promotion of risk assessment tools

*Principal actors: the Ministry of Modernisation, the Norwegian Industrial Safety and Security Organisation, and trade organisations.*

a. Please describe in detail the programmes and resources devoted to the development and promotion of risk assessment tools
b. How are the needs for risk assessment tools evaluated?
c. How is the private sector (corporations, citizens, NGOs) involved?
d. Please describe existing procedures, both public and private, for categorizing information as well as information systems and networks according to their socio-economic criticality and exposure to cyber-threats.

*B. Policy decision-making*

B.1. Strategy co-ordination and supervision

*Principal actors: the KIS and its participating departments and agencies.*

a. The Norwegian Strategy for Information Security is built on a three-tier approach: "defence in depth" for systems of relevance for national security, specific protection of critical infrastructure systems based on public-private co-operation, and the promotion of a culture of safety for the society at large. For each of these tiers, please describe the current competencies and responsibilities in decision-making regarding strategic orientations.
b. For each of these tiers, please describe the current decision-making process. Explain, in particular, how the principal stakeholders (administrations, infrastructure operators, citizens, corporations and NGOs) are involved. If relevant, provide examples of public/private partnerships and cooperation with structures such as ISACs.
c. What is the degree of centralisation of IT security policy in public administrations at present (e.g. totally centralised, common guidelines with sectoral responsibility for their implementation, totally decentralised)? Please make a distinction between the relevant layers of policy (risk assessment, patch management, firewalls and other protections, reporting of incidents, contingency planning, etc.).
d. What is the degree of coordination of IT security policy in critical infrastructures at present (e.g. central monitoring, guidelines, simple communication)? Please make a distinction between the relevant layers of policy (risk assessment, patch management, firewalls and other protections, reporting of incidents, contingency planning, etc.).
e. What changes is the implementation of the National Strategy and the establishment of the KIS expected to bring into the decision-making process?
f. What are the existing capacities for collecting information and conducting analyses on existing information security policies and structures, learning lessons and managing strategic changes?

B.2. Resource allocation for risk management options

*Principal actors: the KIS and its participating departments and agencies.*

a. What are the underlying criteria and principles for determining acceptable levels of risk?

b. How are alternative courses of action (regulations, information campaigns, public/private partnerships, research and development, etc.) considered and compared in the decision-making process?
c. Are cost-benefit analyses carried out for each package of measures *ex ante*? *ex post*? If yes, how are costs and benefits assessed?
d. Are there any planned measures to increase the use of decision support tools such as cost-benefit analysis? Has the government an explicit position regarding the conditions in which such tools could be used in the decision-making process? If yes, please describe.
e. Are the various stakeholders involved in the above steps of decision-making (bullet points a to d)? If yes, please describe how.

*C. Framework conditions*

C.1. Development and use of standards and certification

*Principal actors: Norwegian Accreditation, NSM, the Ministry of Modernisation and the Ministry of Defence.*

a. What are the relative roles of Norwegian Accreditation, SERTIT, and other bodies involved in certification and the promotion of security standards? To what extent and how are these bodies co-ordinated?
b. Is there an established policy with regard to the development of security standards? How have the private sector and other stakeholders been involved in its elaboration?
c. How commonly do Norwegian organisations use national and international standards, such as ISO/IEC 15408 and ISO/IEC 17799?
d. Do public IT procurement policies explicitly refer to security features? If yes, please describe.
e. Do private IT procurement policies make explicit reference to security features? Please provide examples.
f. What are the perceived obstacles to more widespread use of IT-security standards?
g. Please describe government's current and planned actions to encourage the use of standards and certification in the area of cyber-security.

C.2. Promotion of security-enhancing technologies

*Principal actors: the Ministry of Modernisation and the Ministry of Trade and Industry.*

a. Please describe the government's initiatives in support of security-enhancing technologies (public/private partnerships, procurement policies, participation in international projects, etc.)
b. In particular, please describe any activities in the public or private sectors related to development of more secure software (e.g. in R&D, development of methodologies, standards, …)

C.3. Legal and regulatory framework

*Principal actors: the Ministry of Justice and the Police, Sectoral regulatory authorities, trade organisations, the Data Inspectorate and the Ministry of Modernisation.*

a. How does the Ministry of Justice and the Police check for inconsistencies, redundancies, impracticalities and gaps in the vast body of laws and regulations pertaining to information security?
b. How are stakeholders involved in the design of new regulations and the evaluation of existing regulations?
c. How are sector-specific regulations enforced? In critical infrastructure sectors (electricity, telecommunications, etc.), how do regulatory authorities ensure that security requirements are fulfilled?
d. How are, according to the legal and administrative framework, responsibilities defined in the case of a failure of system or network of importance for national security? of a critical infrastructure information system?
e. To what extent are IT vendors and service providers held liable for security defects in their products, systems and networks?
f. Has Norway implemented the EU directives 95/46/EC on data protection and 2002/58/EC on privacy and electronic communications? If yes, how has each of the directives affected legislation on IT security?
g. Are there cases in which a conflict has been perceived between security-enhancing measures planned or taken and the protection of the privacy of employees and/or users? If so, how have these been solved? Please give examples.
h. All in all, how has liability legislation applicable to the security of information products, systems and networks evolved in recent years?

*D. Protection of ICT infrastructure*

D.1. Security of governmental information systems

*Principal actors: Ministry of Modernisation, the Data Inspectorate.*

a. What are the respective competencies and responsibilities of the Ministry of Modernisation and of other entities involved in the protection of governmental information systems and networks (including the operating services themselves)?
b. Are the actions of these entities co-ordinated, and if yes, how?
c. In what ways, if any, do actual practices differ from administrative rules with respect to information security?
d. Who is responsible for testing the security of information systems? What are the methods used (red teaming, penetration tests, etc.)?
e. Are security audits carried out? If so, at which frequency, and which are the main elements of the audit?
f. What are the channels through which operators and users of governmental systems can provide feedback regarding security management?
g. What are the underlying criteria and principles for determining an acceptable level of protection in government services infrastructure?
h. Are cost-benefit analyses carried out to determine the acceptable level of protection?
i. What are the practices inside the government with regard to collection of information about best available technologies and international experiences in the protection of information systems?
j. What are the preliminary and anticipated effects of recent reforms carried in the framework of the National Strategy on the security of governmental information systems and networks? Please describe.

D.2. Security of critical infrastructure information systems

*Principal actors: Ministry of Transport and Communications, Directorate of Social Services and Health, DSB.*

a. Please describe the respective roles and responsibilities of entities involved in the protection of critical information infrastructures, in particular sectoral (e.g. Ministry of Transport and

Communications, Directorate of Social Services and Health) and cross-sectoral (Ministry of Justice and the Police, DSB, NSM) departments of the government, as well as the operators.

b. Are the actions of these entities co-ordinated, and if yes, how?
c. Who is responsible for testing the security of information systems? What are the methods used (red teaming, penetration tests, etc.)?
d. Are security audits carried out? If so, at which frequency, and which are the main elements of the audit?
e. What are the underlying criteria and principles for determining an acceptable level of protection in critical information infrastructure?
f. Are cost-benefit analyses carried out to determine the acceptable level of protection?
g. What are the practices among critical infrastructure operators with regard to collection of information about best available technologies and international experiences in the protection of information systems?
h. To what extent is the private sector and other non-governmental actors integrated in critical information infrastructure protection activities, and is this cooperation coordinated and known to all other government actors in the field?
i. Is there a dialogue between stakeholders (private and public) and governmental bodies concerning needs and preferences in critical information infrastructure protection (similar to ISACs)? Is this dialogue formalised and systematic?
j. What are the preliminary and anticipated effects of recent reforms carried in the framework of the National Strategy on the security of critical information infrastructures? Please describe.

D.3. Research and Development

*Principal actors: Norwegian Research Council, Ministry of Modernisation, Ministry of Justice and the Police, Ministry of Defence, DSB, NSM.*

a. How is R&D in information security organised? Please describe the competencies and responsibilities of all involved entities, both public and private.
b. What is the budget of R&D in information security (amount, percentage of the total R&D budget)?
c. What are the major programmes of R&D in information security?
d. Is there any central coordination of funding and guiding principles for R&D in information security?

e. Does the private sector participate in CIIP R&D projects? Are there reporting practices for such cooperation and is this cooperation coordinated, if so, by whom?
f. Does Norway participate in international R&D projects regarding information security?

D.4. Education

*Principal actors: Ministry of Education and Research.*

a. Is information security covered in national school curricula?
b. To which extent is information security included in general IT education at the university level?
c. Have any specific ICT university programmemes been established (e.g. Masters)?

*E. Information and early warning*

E.1. Awareness-raising

*Principal actors: Ministry of Modernisation, SIS, Norwegian Industrial Safety and Security Organisation and trade organisations, Ministry of Transport and Communications.*

a. Please describe the roles and responsibilities of entities involved in awareness-raising, both in the government (Ministry of Modernisation, SIS, Ministry of Transport and Communications, etc.) and in the private sector (Norwegian Industrial Safety and Security Organisation, NGOs, etc.).
b. Are there any co-operation and co-ordination mechanisms between these entities?
c. To which extent has the objectives of the National Strategy been reached concerning awareness-raising (information campaigns, brochures, websites, etc.) and which are the planned future actions? What have been the results of recent organisational changes (creation of MoM and SIS)?
d. In particular, have there been attempts to measure the impact of campaigns on targeted audiences? If yes, please describe the results.

E.2.Information-sharing

*Principal actors: NSM/NorCERT, SIS.*

a. Please describe the roles and responsibilities of entities involved in information-sharing, in particular in the central government (NSM/NorCERT, SIS) and in the private sector (ISACs?).
b. Are there any co-operation and co-ordination mechanisms between these entities?
c. Are there are legal provisions relating to information-sharing?
d. What are the principal channels of information-sharing with international actors? Which are the most important among these?
e. What have been the results of recent organisational changes (creation of NSM, NorCERT and SIS) for information-sharing?

E.3. Warning

*Principal actors: VDI, SIS, UNINETT CERT, TERT, other CERTs.*

a. Please describe the roles and responsibilities of entities in charge of providing warning, in particular central authorities (VDI, SIS, UNINETT CERT, TERT) and other CERTs.
b. Are there any co-operation and co-ordination mechanisms between these entities? Are the procedures of warning coordinated between the different central authorities?
c. Are any specific measures made to limit the number and impact of false alarms?
d. Is there any mechanism for feedback and learning from past experiences?
e. Are there any established warning and reporting mechanisms between the public and private sectors?
f. Are there any specific warning mechanisms for specific groups, e.g. private persons, small- and medium-sized enterprises without own IT department, etc.?
g. What are the principal channels of information-sharing with international actors? Which are the most important among these?
h. What have been the results of recent organisational changes (SIS, VDI, etc.) for warning?

*F. Rescue*

*Principal actors: UNINETT CERT, TERT, other CERTs.*

a. What entities are competent regarding incident response for information systems of importance for national security? for critical infrastructure information systems? for other systems and networks? In each case, please explain the entity's role, and if relevant, how it co-ordinates its action with other entities (e.g. between different critical infrastructures, or between private and public sectors).
b. What legal or regulatory provisions apply to incident response in information systems of importance for national security? in critical infrastructure information systems? in other systems and networks?
c. What triggers incident response in information systems of importance for national security? in critical infrastructure information systems? in other systems and networks?
d. Is response co-ordinated in advance with the system and network operators? Are there emergency management drills and pre-established communication channels? If yes, please describe and where relevant, make a distinction between systems of importance for national security, critical infrastructures and other systems.
e. How is incident response co-ordinated with warning to prevent further expansion of incidents and attacks?
f. How are incident response needs evaluated and corresponding resources allocated between the competent public entities?

*G. Recovery enhancement*

*Principal actors: DSB, NSM.*

a. What entities are competent for developing contingency and business continuity plans for information systems of importance for national security? for critical infrastructure information systems? for other systems and networks?
b. What are the legal provisions, regulations and guidelines relating to contingency and business continuity plans? Please describe.
c. How does the government encourage the adoption of contingency and business continuity plans?
d. How are information and sound practices shared?
e. What entities are competent for evaluating contingency and business continuity plans for information systems of importance for national security? for critical infrastructure information systems?
f. What are the underlying criteria for developing or evaluating contingency and business continuity plans?
g. How often are contingency and business continuity plans evaluated?

*H. Experience feedback and organisational change*

*Principal actors: SIS, OKOKRIM, KIS.*

a. Are there any institutional mechanisms for evaluating the effectiveness of IT security policies and providing feedback? Please describe.
b. On what grounds are policy measures the evaluated? What quantitative and/or qualitative criteria, if any, are used? Please answer separately for different types of policy.
c. Are stakeholders involved in the evaluation process, and if yes, how?
d. Which other channels exist for the private sector, NGOs or citizens to provide feedback on existing structures and policies? To what extent can these trigger reflections or investigations on a specific issue? Please illustrate.
e. Are there any institutional mechanisms for collecting information on incidents, investigating their sources, and providing feedback? Please describe and if relevant, make a distinction between judiciary enquiries, administrative enquiries, audits, etc.
f. What are the institutional competencies and resources of incident investigation services?
g. Are there past examples where experience feedback has led to organisational change? How is organisational change decided and implemented?
h. How are international practices and experiences used in evaluating and elaborating Norwegian information security policies?

## Annex 4: Members of the Steering Group

**DENMARK:**

Niels JACOBSEN
Head of Section
Danish Emergency Management Agency

Niels MADSEN
Senior Advisor
Danish Emergency Management Agency

Dorte JUUL MUNCH
Head of Section
Civil Sector Preparedness Division
Danish Emergency Management Agency

Henrik Grosen NIELSEN
Head of Division
Emergency Management Division
Ministry of the Interior and Health

Signe RYBORG
Head of Unit
Ministry of the Interior and Health

**FRANCE:**

Geneviève BAUMONT
Secrétaire du Comité de la Prévention et de la Précaution
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

Antoine BOISSON
Bureau de l'évaluation des normes et de la sécurité environnementale
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

Annie ERHARD-CASSEGRAIN
Bureau de l'évaluation des normes et de la sécurité environnementale
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

Emmanuel MASSE
Bureau de l'évaluation des normes et de la sécurité environnementale
Direction des études économiques et de l'évaluation environnementale
Ministère de l'Ecologie et du Développement Durable

**ITALY:**

Andrea SANTUCCI
Directorate for Environmental Protection
Ministry of the Environment and Land Protection

Maria GRAZIA COTTA
Directorate for Soil Defence
Ministry of the Environment and Land Protection

Francesco TORNATORE
Basin Authority of Po river

Donato DI MATTEO
Head of Division for Industrial Risks
Directorate for Environmental Protection
Ministry of the Environment and Land Protection

Alicia MIGNONE
Science Attaché
Permanent Delegation of Italy at the OECD

**JAPAN:**

Kotaro NAGASAWA
Director of Europe Office
Infrastructure Development Institute

Yoshiyuki IMAMURA
Programme Specialist,
Division of Water Sciences, UNESCO

Takashi NAKAJIMA
Deputy- director of Europe Office
Infrastructure Development Institute

Kazuo UMEDA
Director of 2nd Research Department
Infrastructure Development Institute

Masaru KUNITOMO
Assistant Director for International Affairs,
River Planning Division, River Bureau
Ministry of Land, Infrastructure and Transport

Hideki HIRAI
Counsellor For Disaster Management
Cabinet Office

**NORWAY:**

Dagfinn BUSET
Adviser, Emergency Planning Unit
Rescue and Emergency Planning Department
Norwegian Ministry of Justice and the Police

Hilde Bostrøm LINDLAND
Project Manager
Directorate for Civil Protection and Emergency Planning
Ministry of Justice and the Police

Stein HENRIKSEN
Directorate for Civil Protection and Emergency Planning
Ministry of Justice and the Police

Terje-Olav AUSTERHEIM
Directorate for Civil Protection and Emergency Planning
Ministry of Justice and the Police

**SWEDEN:**

Ulf BJURMAN
Head of Department/Director
Swedish Rescue Services Agency

Alf ROSBERG
Project Leader
Swedish Rescue Services Agency

Jim SANDKVIST
Director
SSPA

Oskar HANSSON
Principal Administrative Officer
Swedish Emergency Management Agency

Maria MONAHOV
Research Co-ordinator
Swedish Emergency Management Agency

Louise SIMONSSON
Research Co-ordinator
Swedish Emergency Management Agency

**SWITZERLAND:**

Rudolf A. MÜLLER
Conseiller scientifique
Secrétariat d'Etat à l'économie

**U.S.A.:**

Larry W. ROEDER, Jr.
Policy Advisor on Disaster Management
Bureau of International Organisations
US Department of State

# OECD Studies in Risk Management

# Norway

## INFORMATION SECURITY

Looking back on the disasters of recent years alone (the Indian Ocean tsunami disaster, Hurricane Katrina, terrorist attacks in New York, Madrid and London, avian flu, the 2003 heat wave in Europe), one could be forgiven for thinking that we live in an increasingly dangerous world. A variety of forces are helping to shape the risks that affect us, from demographic evolutions to climate change, through the development of mega-cities and the rise of information technology. These changes are clearly a major challenge for risk management systems in OECD countries, which have occasionally proved unable to protect the life and welfare of citizens or the continuity of economic activity.

The OECD Futures Project on Risk Management Policies was launched in 2003 in order to assist OECD countries in identifying the challenges of managing risks in the 21st century, and help them reflect on how best to address those challenges. The focus is on the consistency of risk management policies and on their ability to deal with the challenges, present and future, created by systemic risks. The Project covers a range of risk management issues which were proposed by the participating countries and together form three thematic clusters: natural disasters, risks to critical infrastructures, and the protection of vulnerable population groups. In the first phase of the Project,
the OECD Secretariat prepared a case study for each issue. The studies cover both recent international developments of interest and the national policy context, and come with a tool for self-assessment to be used later in the Project in order to review the national policies in question.

This work is now published as the OECD Studies in Risk Management.

www.oecd.org