OECD Reviews of Risk Management Policies

Norway

INFORMATION SECURITY

OECD

OECDPUBLISHING

OECD Reviews of Risk Management Policies

Norway

INFORMATION SECURITY

OECD

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

Foreword

The OECD review of risk management policies in Norway concerning information security is the first country review conducted in the framework of the OECD Futures Project on Risk Management Policies. Launched in October 2003, this is a pilot project that brings together OECD Member Countries willing to share their knowledge and experiences in identifying and addressing the challenges of managing risks in the 21st century. The project is monitored by a steering group consisting of the representatives of participating ministries and agencies. It follows a multi-disciplinary approach and covers themes as varied as natural disasters, critical infrastructures, and vulnerability reduction for particular segments of the population. The focus is on the consistency of risk management policies and on their ability to detect, and adapt to, changes in the risk landscape. The country reviews are based on a background study prepared, discussed and adopted during the first phase of the project, a self-assessment of policy by national authorities using an ad-hoc questionnaire, and a series of interviews carried out in the country by the OECD review teams.

The review of Norway's policies regarding information security was set up at the request of the Norwegian Ministry of Justice and the Police, to, in the ministry's words, "aid national authorities and the new National Information Security Coordination Council in refining and developing focussed (…) measures and policies aimed at reducing vulnerabilities". To support the process, the ministry's Directorate for Civil Protection and Emergency Planning (DSB) organised two workshops in Oslo in March 2004 and April 2005, bringing together a large number of national entities involved in the management of information security. In June 2005, the OECD review team conducted a set of interviews with representatives from a number of ministries and agencies of the Norwegian government, the business sector and non-governmental organisations. The team submitted an interim report of findings and recommendations to the Norwegian authorities in September 2005, and a first draft of this report in November 2005.[1]

The policy analysis in this report seeks to identify areas where good practices are evident, as well as areas where improvements could be made. With respect to the latter, opportunities for action are proposed and alternatives are suggested when possible. In doing so, the report tries to respond to the initial request of the Ministry of Justice and the Police, while

[1] This final report is both broader in scope and more in-depth than the interim report. Its recommendations are therefore more elaborate, slightly more numerous, and presented in a different order to that of the interim report.

at the same time acknowledging the difficulty of constructing a coherent, complete and effective policy approach in this emerging field of policy-making.

The ministry's mandate focussed on vulnerability reduction, leaving aside some elements of security management, notably the identification, assessment, monitoring and deterrence of threats. These areas of policy are therefore beyond the scope of this report.

The team that carried out the review and prepared this report was led by Nick Mansfield, an independent expert, and was composed of Ronald van der Luit, from the Netherlands Ministry of Economic Affairs, Matthieu Grall, from France's Secrétariat Général de la Défense Nationale, and Reza Lahidji and Marit Undseth, from the OECD Secretariat.

The team is indebted to Stein Henriksen, at the Norwegian Directorate for Civil Protection and Emergency Planning, for his wise counsel. The team would also like to thank all those in Norway who contributed to the review process through interviews, comments and supply of information.

This report is issued under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

Summary of Findings and Recommendations

Norway has a well-developed set of policies, institutions and laws to preserve and improve the security of information systems and networks. In addition, since the end of the 1990s the country has taken several major initiatives in this area, which have modernised the legal and institutional context. The bulk of the existing tools to protect information security are specific to sectors such as communications, banking and finance, energy, etc. The OECD review of Norway's information security policies placed particular emphasis on the definition of a "security baseline" for these sectoral approaches, and on co-ordination issues. The aim of this executive summary is to highlight the major findings, opportunities for action and recommendations put forward by the review, focussing in particular on remaining weaknesses and areas for improvement.

Chapter 1. The Norwegian Strategy for Information Security

Findings

The review of the National Strategy for Information Security and its implementation shows a number of strong points and some opportunities for improvement. With regard to its scope and objectives, the Strategy outwardly covers the broad spectrum of information security management issues, stating in particular that "critical IT infrastructures shall be protected in terms of availability, integrity and confidentiality." When it comes to the actual tools of security policy, however, the availability and integrity of information is highly dependent on sectoral approaches. At the cross-sector level, the approach seems focussed on protecting the confidentiality of classified information, and the emphasis on defining a baseline in terms of availability and integrity is less than adequate. The co-ordination and control mechanisms in place show the same tendency, as the entities in charge of co-ordinating security measures for non-classified information do not seem to have the necessary authority to fulfill all of their formal responsibilities. Finally, while the implementation of the Strategy follows a learning approach and is well-adapted to the reality of information security management, there are opportunities to strengthen the monitoring, feedback and appraisal of implementation measures.

Opportunities for action

- The policy options to sharpen the focus on availability and integrity include correcting the imbalance in the Act Relating to Protective Security Services among security, availability and integrity, via new legislation currently under consideration regarding the protection of objects and assets. This would entail extending the scope of the Act from classified information and systems to include information and systems of relevance for the nation's security and societal welfare (e.g., critical infrastructures).

- Assignment of responsibility could be improved regarding the management of non-classified information, in particular in areas such as the co-ordination of ministerial initiatives, the provision of standards and guidelines for "fault tolerant" systems, and backup and disaster recovery procedures. These could be set at a general level as part of promoting the concept of a baseline of minimum national preparedness (this issue is addressed in more detail in Recommendation 5).

- The role of civil actors in developing information security policies could be strengthened. The knowledge and expertise of a broad range of actors from the military/law enforcement and civil sectors is needed in order to clarify concepts such as "critical infrastructures", "societal security" and "continuity of supply", and to organise risk management activities accordingly (see also Recommendation 6).

- The learning approach to the implementation or improvement of the Strategy could be enhanced by setting detailed objectives for each ministry, measuring progress towards these objectives, and appraising the overall performance of the information security management system in the prevailing risk situation on a regular basis.

Recommendation 1: Develop the appropriate tools and improve the sharing of responsibility for information security policy in order to better address availability and integrity needs.

Recommendation 2: Elaborate a performance appraisal process to measure the effectiveness of current information security control processes against current threats.

Chapter 2. Assessing Information Security Risks

2.1. Risk assessment in the government

Findings

Risk assessment regarding government systems is incomplete. A general standard has been adopted for the government, but is not implemented as a security baseline, and therefore cannot help to simplify the challenging task of assessing risks to government systems.

In the absence of a complete and consistent assessment of risks, it is difficult to assign comprehensive responsibility for security management, and set priorities for government action.

Opportunities for action

- Norway could initiate a project to implement an information security management standard such as ISO 17799 as a security baseline in all government IT-related activities. Based on the experience of other governments and large organisations, a gradual process of implementation could be defined: Norwegian ministries could for instance aim to achieve self-declared compliance with the standard within five years; then a formal certification in the Norwegian accreditation scheme would be requested within ten years. Such a systematic approach would have the advantage of setting an example for the private sector.

- In addition, Norwegian internal and third party IT contracts could contain a requirement for demonstrated compliance with relevant information security standards and guidelines. Norwegian internal and third party network connection agreements could also contain a requirement for demonstrated compliance with relevant information security standards and guidelines.

- The National Security Authority (NSM) could provide Common Criteria Protection Profiles for certified products and systems that are also consistent with information security management defined by ISO 17799 to meet the requirements of the Act Relating to Protective Security Services.

- A ministerial level risk assessment could detail security requirements and clarify the "rules of the game" for implementing a security management standard as a baseline. Some of these requirements could be defined by compliance with general government security laws, data protection laws and the like. Others could aim at ensuring continuity of supply of essential services in the ministry's sector.

Recommendation 3: Define and implement a baseline approach to security management in government systems, complemented by focussed risk assessments.

2.2. Risk assessment in critical infrastructures

Findings

Risk assessment regarding critical information infrastructures is incomplete, but the BAS5 project, and especially the work of the government commission on critical infrastructures, might provide a solid basis for it.

Opportunities for action

- As a follow-up to the work of the government Commission on Critical Infrastructures, a process of dialogue among users, suppliers and regulators of critical infrastructures could be developed across sectors, in order to clarify issues of risk assessment, in particular with regard to information security (see also Recommendation 6).

- The opportunity could also be offered to users and suppliers of critical infrastructures to make inputs to the BAS5 project (see also Recommendation 13).

Recommendation 4: Put in place a systematic process of risk assessment for critical infrastructures.

Chapter 3. Protecting Information Systems

3.1. Protection of government systems

Findings

Responsibility with regard to information security policy is scattered across too many ministerial stakeholders to be carried out consistently.

Opportunities for action

- Norway could consider alternative ways to achieve a more co-ordinated national information security policy. One option could be to assign a clear leadership role to a single ministry on all information security issues beyond the present scope of the Act Relating to Protective Security Services, with a mandate to develop information security as an integrated part of e-government and e-business. This could reduce any duplication of initiatives carried out within different ministries and focus efforts on priority issues.

- Another possibility could be to co-ordinate policies regarding information security at cabinet level (as proposed in Recommendation 10 regarding the management of emergencies). Following this model, individual ministries could then take responsibility for the execution of priority actions and delivering the actual improvements.

- An alternative which would be compatible with a decentralised architecture would be to clearly set standards defining the baseline approach at a central level, then monitor and enforce their implementation through management and performance appraisals in the government audit processes.

Recommendation 5: Allocate responsibility among a smaller number of players inside the government.

3.2. Protection of critical infrastructure systems

Findings

Two main challenges in relation to critical infrastructure protection have been identified: first, to clarify the division of responsibilities for critical infrastructure protection between government and operators, including for the handling of interdependencies among infrastructures; second, to communicate and co-operate with all critical infrastructure owners and operators in a systematic way.

Opportunities for action

- In order to facilitate regular communication and co-operation, the government could make a general overview of critical infrastructures actors, large and small, and their security situation (for instance in relation with the BAS5 project).

- A systematic cross-sector dialogue involving the government and operators and users of critical infrastructures (as sketched in Recommendation 4) could address the questions of risk acceptability in critical infrastructures, and of the level of security that operators have to ensure as part of their normal business. The output from this dialogue could be a clear allocation of responsibilities among operators, regulators and supervisory bodies regarding Critical Infrastructures Protection (CIP), established in a broader context than regulatory market oversight.

- Various mechanisms could be put in place to ensure that due diligence is respected in critical infrastructures, from liability laws and economic incentives to mandatory audits and benchmarking exercises.

- Responsibility and authority could additionally be assigned for the management of interdependencies and issues concerning continuity of supply that fall beyond the scope of sector regulators, in co-operation with these regulators.

Recommendation 6: Determine risk acceptability and the sharing of responsibility in risk management for each critical infrastructure.

Recommendation 7: Strengthen the involvement of operators in risk management activities.

Chapter 4. Managing Incidents, Emergencies and Crises

4.1. Incident management

Findings

While the impact of a major information security crisis on SMEs and on society as a whole would probably be considerable, there are few incentives for the private sector to create an incident response function.

Opportunities for action

To address this capacity gap it is suggested that the Norwegian government create a CERT (Computer Emergency Response Team) specifically aimed at the needs of the private sector, in particular SMEs, in connection with the SIS (Senter for informasjonssikring – Centre for Information Security) and the NSO (Næringslivets sikkerhetsorganisasjon - Industrial Safety and Security Organisation) (see Recommendation 11).

Recommendation 8: Encourage the development of incident response support for SMEs.

4.2. Contingency and preparedness planning

Findings

There is a gap in responsibility regarding consultancy and audit of contingency planning for private critical infrastructures and public services that do not manage classified information.

Two major candidates for giving advice on information security preparedness, contingency planning and threat scenarios, namely NSM and DSB, are also in charge of audits.

Opportunities for action

- The government could develop a consultancy capability for users in the public and private sectors in order to encourage the creation of contingency plans.

- A government auditing function could be extended to include critical infrastructures, irrespective of whether they are publicly or privately owned or operated, and whether they manage classified or non-classified information. Private audits could also be used.

- In parallel, the government could also consider the principle of separation of the audit and consultancy functions, which has become commonplace and often mandatory in the private sector.

Recommendation 9: Strengthen government consultancy and auditing services in order to promote preparedness and contingency planning.

4.3. Emergency and crisis management

Findings

A centre for national crisis management can play a vital role in monitoring an IT crisis as it develops and in mitigating the effects if it develops beyond the stages of incident or emergency.

Opportunities for action

To be most effective the “core” members of a centre for national crisis management should have the collective authority to direct and manage resources once a crisis has been declared. This authority and the declaration of such a crisis may need to be supported by Parliament and relevant crisis management legislation. This centre could be a component of the newly created Cabinet Emergency Council (see also Recommendation 5).

Recommendation 10: Create a national IT crisis management capability.

Chapter 5. Strengthening the Foundations of Security

5.1. Awareness-raising

Findings

Awareness-raising is effective only if accompanied by incident support and the promotion of solutions. In this respect the launch of the NettVett website and the decision to make SIS a permanent organisation primarily oriented towards SMEs are positive steps.

Opportunities for action

- In order to sustain recent progress in the outreach to small businesses and the general public, the authorities could put the funding of SIS and NettVett on a sound, long-term footing.

- Partnerships could be developed through SIS in order to support outreach to business and civil society.

- The creation of a CERT-type structure dedicated to SMEs could help to promote solutions at the same time as increasing awareness about risks (see Recommendation 8).

Recommendation 11: Improve and rationalise awareness-raising efforts directed towards SMEs and the general public.

5.2. Information-sharing

Findings

There is a fair amount of knowledge and experience of information security in individual ministries and agencies, but opportunities to share this knowledge are restricted in some cases by the existence of sector-specific ministerial “silos”. Improvements could be made in stimulating the exchange of information and best practices among users on how to secure their networks and information systems, according to their individual level of maturity regarding information security.

Opportunities for action

- A low-cost option for providing support platforms for SMEs would be to sponsor, encourage and promote small, local self-help groups, supported with external advice from experts in government and universities.

- The roles of open and closed forums could be more clearly differentiated according to the level and sensitivity of information exchanged.

- SIS and NorCERT could be used as more active and wide-ranging platforms for information-sharing for all types of end users, with specific tools for different target groups: individuals, SMEs, public administrations, etc. (see also Recommendation 11).

Recommendation 12: Stimulate the exchange of information and best practices among users.

5.3. Education and R&D

Findings

The connection between research and the Norwegian information security strategy is tenuous, and the ultimate beneficiaries of research seem to have limited possibilities to influence the content of research programmes.

Where research programmes are oriented towards a specific issue or solution, their monitoring could be better facilitated if the programmes included an exploitation plan from the outset. The expected benefits and beneficiaries would thus be more clearly identified. The BAS5 project seems to suffer from the lack of such requirements, which possibly explains the gradual changes in its content, objectives, and resources.

Opportunities for action

- Information-sharing with the relevant government departments and agencies could be a mandatory condition of any research sponsorship agreement in this area. Such connections were not found in either of the research initiatives considered.

- A national strategy on information security research would help to identify gaps, prioritise resources, guide research programmes and identify areas where co-operation with foreign counterparts might add most value.

- Potential users and the beneficiaries of research could be given a greater role in the definition and guidance of research programmes. The KIS is one possible forum for this type of activity, provided that the private sector is more specifically involved. The KIS could also be given the opportunity to commission, fund and evaluate research, in order to make more use of the demand side to guide research programmes.

Recommendation 13: Define a national strategy on information security research, and enhance the role of the demand side in guiding research projects.

Synthèse des conclusions et recommandations

La Norvège dispose d'un vaste ensemble de politiques, d'institutions et de lois pour préserver et améliorer la sécurité des systèmes et réseaux d'information. En outre, la Norvège a engagé depuis la fin des années 1990 plusieurs mesures importantes qui ont permis de moderniser l'architecture législative et institutionnelle dans ce domaine. L'essentiel des outils existants pour protéger la sécurité de l'information est spécifique à certains secteurs d'activité : communications, banque et finance, énergie, etc. L'examen par l'OCDE des politiques de la Norvège en matière de sécurité de l'information fait ressortir la nécessité de définir un « niveau minimum » de sécurité pour ces approches sectorielles, et pointe quelques problèmes de co-ordination. L'objectif de cette synthèse est de présenter les principales conclusions, opportunités d'action et recommandations qui ressortent de l'examen, en prêtant une attention particulière aux lacunes qui subsistent et aux points qui restent à améliorer.

Chapitre 1. Stratégie de la Norvège en matière de sécurité de l'information

Conclusions

L'examen de la stratégie nationale en matière de sécurité de l'information et de sa mise en œuvre fait apparaître un certain nombre de points forts, mais aussi des aspects qui pourraient être améliorés. Si l'on s'intéresse à son champ d'application et à ses objectifs, la stratégie semble répondre à tous les problèmes de gestion de la sécurité de l'information ; il est précisé en particulier que « les infrastructures critiques des technologies de l'information (TI) doivent être protégées quant à leur disponibilité, leur intégrité et leur confidentialité ». Toutefois, s'agissant des outils de cette politique de sécurité, l'attention portée à la disponibilité et à l'intégrité de l'information varie selon les secteurs d'activité. L'approche transversale semble pour sa part centrée sur la protection de la confidentialité des informations classifiées, et l'importance de la définition d'un niveau minimum s'agissant de la disponibilité et de l'intégrité n'y est pas suffisamment reconnue. Cette observation vaut aussi pour les mécanismes de coordination et de contrôle en place : les entités chargées de coordonner les mesures de sécurité pour les informations non classifiées ne semblent pas avoir les pouvoirs nécessaires pour s'acquitter de la totalité de leurs responsabilités formelles. Enfin, si la stratégie suit un processus d'apprentissage bien adapté aux réalités de la gestion de la sécurité de l’information, il serait possible de renforcer ce processus en améliorant certaines fonctions de surveillance et d’évaluation de la mise en œuvre des mesures, et de retour d’expérience.

Opportunités d’action

- Pour donner davantage de poids aux aspects de disponibilité et d’intégrité des systèmes, il serait souhaitable, à travers la nouvelle législation actuellement en discussion, de rectifier le déséquilibre entre sécurité, disponibilité et intégrité qui existe dans la Loi relative aux services de protection de la sécurité. Il faudrait pour cela élargir le champ d’application de la Loi au delà des informations et des systèmes classifiés, et y inclure les informations et systèmes ayant une importance du point de vue de la sécurité de la nation et du bien-être de la société (en particulier les infrastructures critiques).

- S’agissant de la gestion des informations non classifiées, la répartition des responsabilités pourrait être améliorée, en particulier dans la coordination des initiatives ministérielles, la création de normes et de lignes directrices sur la robustesse des systèmes, et les procédures de sauvegarde et de reprise après des sinistres informatiques. Elles pourraient s’appliquer à l’ensemble des secteurs dans le cadre de l’application du concept de niveau national de préparation minimum (cet aspect est traité plus en détail dans la recommandation 5).

- Le rôle de la société civile dans l’élaboration des politiques de sécurité de l’information pourrait être renforcé. Le savoir et l’expertise d’une large gamme d’acteurs – armée, police, société civile – sont nécessaires pour définir clairement des concepts tels que « infrastructures critiques », « sécurité de la société » et « continuité d’approvisionnement » et pour organiser la gestion du risque en conséquence (voir aussi la recommandation 6).

- L’approche graduelle dans la mise en œuvre et l’amélioration de la stratégie pourrait être renforcée en fixant des objectifs détaillés pour chaque ministère, en mesurant les progrès accomplis vers ces objectifs, et en évaluant régulièrement la performance globale du système de gestion de la sécurité de l’information au regard de la configuration de risque effective.

Recommandation 1 : Mettre au point les outils nécessaires et améliorer le partage des responsabilités pour la politique de la sécurité de

l'information afin de mieux répondre aux exigences de disponibilité et d'intégrité.

Recommandation 2 : Élaborer un processus d'évaluation de la performance afin de mesurer l'efficacité des processus de contrôle de la sécurité de l'information au regard des menaces existantes.

Chapitre 2. Évaluer les risques pesant sur la sécurité de l'information

2.1. Évaluation des risques au sein de l'administration

Conclusions

L'évaluation des risques pesant sur les systèmes gouvernementaux n'est pas complète. Une norme globale pour l'administration a été adoptée mais elle n'est pas appliquée comme mesure minimum de sécurité, et ne peut donc pas contribuer à simplifier la tâche délicate de l'évaluation des risques pour les systèmes administratifs.

En l'absence d'une évaluation complète et cohérente des risques, il est difficile d'identifier et d'attribuer toutes les responsabilités dans la gestion de la sécurité, et d'établir des priorités pour l'action des pouvoirs publics.

Opportunités d'action

- La Norvège pourrait s'engager dans la mise en place d'une norme en matière de gestion de la sécurité (telle que ISO 17799) comme mesure minimum pour toutes les applications informatiques de l'administration. En s'appuyant sur l'expérience des administrations d'autres pays et de grandes organisations, un processus de mise en œuvre progressive pourrait être défini : les ministères norvégiens pourraient par exemple viser l'auto-déclaration de conformité à la norme dans les cinq ans : ensuite, une certification officielle dans le cadre d'un dispositif national d'accréditation serait requise dans les dix ans. Cette approche systématique aurait l'avantage de pouvoir servir d'exemple au secteur privé.

- En outre, les contrats internes à l'administration et avec les entreprises sous-traitantes pourraient contenir une clause sur la conformité avec les normes et les principes directeurs pertinents en matière de sécurité de l'information. En matière de liaisons réseau, accords internes à l'administration et avec des entreprises sous-traitantes pourraient également contenir un impératif de démonstration de conformité avec les normes et principes directeurs pertinents en matière de sécurité de l'information.

- Le NSM pourrait définir des profils de protection relatifs aux Critères communs (ISO 15408) pour les produits et systèmes certifiés qui soient aussi conformes aux règles de gestion de la sécurité définies dans la norme ISO 17799 pour répondre aux impératifs de la Loi relative aux services de protection de la sécurité.

- Une évaluation du risque au niveau ministériel pourrait établir en détail des impératifs de sécurité et clarifier les « règles du jeu » pour la mise en œuvre d'une norme de gestion de la sécurité en tant que mesure minimum. Une partie de ces impératifs pourraient être définis par la conformité avec les lois générales de sécurité s'appliquant dans l'administration, les lois de protection des données, etc. D'autres pourraient avoir pour objectif d'assurer la continuité de fourniture des services essentiels dans le secteur du ministère.

Recommandation 3 : Définir et mettre en œuvre une approche minimum dans la gestion de la sécurité dans les systèmes de l'administration, complété par des évaluations ciblées du risque.

2.2. Évaluation du risque dans les infrastructures critiques

Conclusions

L'évaluation du risque pesant sur les infrastructures de l'information critiques n'est pas complète, mais le projet BAS5 et surtout les travaux de la commission gouvernementale sur les infrastructures critiques pourraient constituer une base solide pour ce travail.

Opportunités d'action

- Dans le prolongement des travaux de la commission gouvernementale sur les infrastructures critiques, un processus de dialogue entre les utilisateurs, les fournisseurs et les régulateurs des infrastructures critiques pourrait être mis au point pour l'ensemble des secteurs, afin de clarifier les aspects de gestion du risque, en particulier concernant la sécurité de l'information (voir aussi la recommandation 6).

- Les utilisateurs et fournisseurs des infrastructures critiques pourraient aussi être invités à apporter une contribution au projet BAS5 (voir aussi recommandation 13).

Recommandation 4 : Mettre en place une procédure systématique d'évaluation des risques pour les infrastructures critiques.

Chapitre 3. Protéger les systèmes d'information

3.1. Protection des systèmes administratifs

Conclusions

Les responsabilités relatives à la politique de sécurité de l'information sont dispersées entre un trop grand nombre d'acteurs ministériels pour être assumées de manière cohérente.

Opportunités d'action

- La Norvège pourrait envisager d'autres solutions pour mieux coordonner sa politique nationale de sécurité de l'information. Par exemple, il serait possible d'attribuer clairement un rôle d'orientation à un ministère donné sur tous les aspects de la sécurité de l'information au-delà du champ d'application actuel de la Loi relative aux services de protection de la sécurité, avec pour mandat de développer la sécurité de l'information comme faisant partie intégrante de l'administration en ligne et de l'électronique d'entreprise. Cela permettrait de réduire le risque de mesures redondantes entre différents ministères et de cibler les efforts sur les aspects prioritaires.

- Il serait aussi possible de coordonner les politiques relatives à la sécurité de l'information au niveau du Cabinet (à l'image de la solution proposée dans la recommandation 10 pour la gestion des urgences). Dans ce modèle, les différents ministères pourraient ensuite assumer la responsabilité d'exécution des tâches prioritaires et de production effective des améliorations.

- Une alternative qui serait compatible avec une architecture décentralisée consisterait à fixer à un niveau central les seules normes définissant une approche minimale, le suivi et l'application étant effectués au moyen d'évaluations de la gestion et de la performance dans le cadre des procédures d'audits de l'administration.

Recommandation 5 : Répartir les responsabilités entre un plus petit nombre d'acteurs au sein de l'administration.

3.2. Protection des systèmes d'infrastructure critiques

Conclusions

Deux grands chantiers restent ouverts en matière de protection des infrastructures critiques ; d'abord, de clarifier la division des responsabilités de protection des infrastructures critiques entre l'administration et les opérateurs, notamment au niveau du traitement des interdépendances entre infrastructures ; ensuite, d'instaurer une communication et une coopération systématiques avec les propriétaires et les opérateurs de toutes les infrastructures critiques.

Opportunités d'action

- Pour faciliter une communication et une coopération régulières, les pouvoirs publics pourraient commencer par dresser un tableau général de tous les acteurs des infrastructures critiques, quelle que soit leur taille, en décrivant leur situation en matière de sécurité (par exemple en relation avec le projet BAS5).

- Un dialogue systématique et plurisectoriel entre l'administration, les opérateurs et les utilisateurs des infrastructures critiques (comme décrit dans la recommandation 4) pourrait répondre aux questions sur le niveau de risque acceptable dans les infrastructures critiques, et du niveau de sécurité que doivent assurer les opérateurs dans le cadre de leur activité normale. Ce dialogue pourrait déboucher sur une répartition claire des responsabilités entre opérateurs, autorités de régulation et organes de supervision en matière de protection des infrastructures critiques, établi dans un contexte plus large que celui de la surveillance réglementaire des marchés.

- Différents mécanismes pourraient être mis en place pour assurer le respect de la règle de droit en matière d'infrastructures critiques : lois en matière de responsabilité, incitations économiques, audits obligatoires, benchmarking.

- Les responsabilités et les compétences pourraient de plus être établies pour les problèmes de gestion des interdépendances et de continuité de fourniture qui sortent du champ de compétence des régulateurs sectoriels, en coopération avec ceux-ci.

Recommandation 6 : Déterminer le niveau de risque acceptable et le partage des responsabilités dans la gestion des risques de chaque infrastructure critique.

Recommandation 7 : Renforcer l'implication des opérateurs dans les activités de gestion des risques.

Chapitre 4. Gérer les incidents, les urgences et les crises

4.1. Gestion des incidents

Conclusions

Une crise majeure de sécurité de l'information aurait sans doute un impact considérable sur les PME et sur la société dans son ensemble ; il existe pourtant peu de mesures pour inciter le secteur privé à mettre en place une fonction de réponse aux incidents.

Opportunités d'action

Pour combler ce déficit de capacité, il est suggéré que le gouvernement norvégien crée un CERT (Centre d'alerte et de réaction aux urgences informatiques) spécifiquement axé sur les besoins du secteur privé, et en particulier sur ceux des PME, en relation avec le SIS et le NSO (voir recommandation 11).

Recommandation 8 : Favoriser le développement d'un système de soutien à la gestion des incidents pour les PME.

4.2. Planification des urgences et préparation

Conclusions

Il existe un déficit de responsabilité dans les fonctions de conseil et d'audit de la planification d'urgence pour les infrastructures critiques privées et les services publics qui n'ont pas à traiter d'informations classifiées.

Deux organismes, le NSM et le DSB, pourraient dispenser des avis sur le niveau de préparation en matière de sécurité, la planification des urgences et les scénarios de menace. Ils sont aussi chargés des audits.

Opportunités d'action

- Les pouvoirs publics pourraient développer une capacité de conseil pour les utilisateurs des secteurs public et privé afin d'encourager à la création de plans d'urgence.

- Une fonction administrative d'audit pourrait être étendue à toutes les infrastructures critiques, que leurs propriétaires ou leurs exploitants soient publics ou privés, et qu'elles aient à traiter des informations classifiées ou non. Les audits pourraient aussi être confiés au secteur privé.

- Parallèlement, les pouvoirs publics pourraient aussi envisager d'appliquer le principe de séparation des fonctions d'audit et de conseil, dont l'usage est devenu courant (voire obligatoire) dans le secteur privé.

Recommandation 9 : Renforcer les services publics de conseil et d'audit afin d'améliorer le niveau de préparation et la planification d'urgence.

4.3. Gestion des urgences et gestion de crise

Conclusions

Un centre national de gestion des crises peut jouer un rôle vital dans le suivi d'une crise de TI à mesure qu'elle se développe, et atténuer ses effets si elle dépasse le stade de l'incident ou de l'urgence.

Opportunités d'action

Pour plus d'efficacité, il faut que les membres-clés d'un centre national de gestion de crise aient une compétence collective de direction et de gestion des ressources une fois qu'une situation de crise est déclarée. Il peut être nécessaire que cette compétence et la déclaration d'une situation de crise s'appuient sur le Parlement et sur une législation spécifique. Ce centre pourrait être une composante du Conseil d'urgence du Cabinet, nouvellement créé (voir aussi recommandation 5).

Recommandation 10 : Créer une fonction nationale de gestion des crises de TI.

Chapitre 5 : Renforcer les fondements de la sécurité

5.1. Sensibilisation

Conclusions

Les actions de sensibilisation ne sont utiles que si elles sont accompagnées d'un soutien en cas d'incidents et si des solutions sont proposées. A cet égard, le lancement de NettVett et la décision de faire de SIS une organisation permanente essentiellement tournée vers les PME sont deux mesures positives prises au cours des derniers mois.

Opportunités d'action

- Pour soutenir les progrès récents accomplis en direction des petites entreprises et du grand public, les autorités pourraient assurer la viabilité de SIS et de NettVett en pérennisant leur financement.

- Des partenariats pourraient être développés avec SIS pour renforcer les actions en direction des entreprises et de la société civile.

- Enfin, la création d'une structure de type CERT dédiée aux PME pourrait contribuer à promouvoir des solutions tout en développant la sensibilisation à l'égard des risques (voir recommandation 8).

Recommandation 11 : Améliorer et rationaliser les actions de sensibilisation en direction des PME et du grand public.

5.2. Partage des informations

Conclusions

Il existe au sein des différents ministères et agences un savoir et une expérience considérables en matière de sécurité de l'information, mais les occasions de partager ces connaissances sont limitées dans certains cas en raison de « silos » sectoriels existant au sein des ministères. Il serait souhaitable de stimuler les échanges d'informations et de bonnes pratiques entre utilisateurs sur les moyens de sécuriser les réseaux et systèmes d'informations, en fonction de leur niveau individuel de maturité en matière de sécurité de l'information.

Opportunités d'action

- Une option économique pour fournir des plates-formes de soutien aux PME consisterait à parrainer, à encourager et à promouvoir de petits groupes locaux d'entraide, avec le soutien et les conseils d'experts extérieurs issus de l'administration et des universités.

- Le fonctionnement et les rôles des forums ouverts et fermés pourraient être plus clairement différenciés en fonction du niveau de sensibilité des informations échangées.

- SIS et NorCERT pourraient être utilisés pour offrir des plates-formes plus actives et plus larges de partage de l'information pour tous types d'utilisateurs, avec des outils spécifiques pour les différents groupes cibles : particuliers, PME, administrations publiques, etc. (voir aussi recommandation 11) ;

Recommandation 12 : Stimuler les échanges d'information et de bonnes pratiques entre utilisateurs.

5.3. Enseignement et R&D

Conclusions

Les liens entre la recherche et la stratégie nationale norvégienne en matière de sécurité de l'information sont particulièrement ténus ; les bénéficiaires finals de la recherche semblent avoir peu de moyens pour influencer le contenu des programmes de recherche.

Lorsque les programmes de recherche sont orientés vers une question ou une solution particulières, leur suivi pourrait être facilité si un plan d'exploitation des programmes était établi dès leur conception. Cela permettrait de définir plus clairement les retombées escomptées et les bénéficiaires des recherches. C'est cette démarche qui semble faire défaut à un projet comme BAS5, ce qui pourrait expliquer le glissement graduel de son contenu, de ses objectifs et de ses ressources.

Opportunités d'action

- Le partage d'information avec les départements ministériels et les agences concernées devrait être une condition obligatoire à tout accord de parrainage de recherches dans ce domaine. De telles relations n'ont pas été observées dans les initiatives de recherche examinées.

- Une stratégie nationale pour la recherche en matière la sécurité de l'information permettrait d'identifier les lacunes, de définir les priorités pour l'attribution des ressources, d'orienter les programmes de recherche et de mettre en évidence les domaines où la coopération avec des équipes étrangères pourrait être la plus fructueuse.

- Les utilisateurs et les bénéficiaires potentiels de la recherche pourraient avoir davantage de poids dans la définition et l'orientation des programmes de recherche. Le KIS est un cadre possible pour ce type de rencontre, à condition que le secteur privé soit associé plus spécifiquement. Le KIS pourrait aussi avoir la possibilité de commanditer, de financer et d'évaluer des recherches, afin de donner plus d'importance à la demande dans l'orientation des programmes de recherche.

Recommandation 13 : Définir une stratégie nationale de recherche sur la sécurité de l'information et renforcer l'influence de la demande dans l'orientation des projets de recherche.

Chapter 1. The Norwegian Strategy for Information Security

Information security is a new field for government policy. To date, the development of information technology and networks (in particular the Internet) has been driven primarily by market forces. Over the past fifteen years, however, the gradual rise in the frequency of malicious acts and their actual or potential impact on OECD economies and societies have made a strong case for government action in the area of information security. All OECD countries have engaged actions to address the challenges of information security in recent years, and many are considering taking additional measures in the not-too-distant future.

These policies face a number of important challenges. First, unlike other fields of risk management where policy tools and institutions exist and have to be gradually adapted to a changing environment, the instruments of information security policy have to be created from scratch for every stage of security management, from the assessment of risks to emergency response, through awareness-raising, information-sharing and the protection of particular systems. Considering the speed of change in technology and applications, and also in the risk environment, even new policy measures can become outdated rapidly. Public policies therefore need to be kept under constant institutional scrutiny, and to be re-oriented, improved or rationalised if need be, before they produce undesirable effects. Moreover, policy measures concern a host of stakeholders operating at different geographical scales, from end users (individuals, businesses, administrations) to access providers, application suppliers, network operators, etc.

This complexity makes it imperative for governments to develop their policy measures in the framework of an overall strategy, in order to ensure consistency and completeness, and to improve the understanding of policy for all stakeholders. Defining and implementing a consistent, comprehensive strategy to enhance information security is a serious challenge in itself, and an ongoing task in most if not all OECD countries. It entails establishing a scope and ultimate goals which are clearly stated and accepted by all parties; describing how to achieve the goals, by creating adequate controls and assigning the corresponding roles and responsibilities; and proposing a roadmap with milestones, evaluation criteria, and feedback mechanisms.

In Norway, the overall framework for information security policy is set by the National Strategy for Information Security. This chapter describes the origins and salient features of the Strategy (Section 1); proposes an assessment of its strengths and weaknesses according to these three elements – scope and objectives, controls and responsibilities, and roadmap and feedback (Section 2); and makes recommendations for action (Section 3).

1.1. Overview of the Strategy

1.1.1. Origins

Norway's Strategy for Information Security was inspired by two important reports issued in 2000: the report of the Government Commission on the Vulnerable Society (Norwegian Ministry of Justice and the Police, 2000), and the Ministry of Trade and Industry's report on information security (Norwegian Ministry of Trade and Industry, 2000). Both highlighted the emergence of information security as a risk area of critical importance, and made recommendations for a strengthened policy approach to it. The numerous legislative and institutional developments in the area of information security since the late 1990s (in particular the Act Relating to Protective Security Services, adopted in 1998) made the need for an overall policy framework all the more urgent.

The elaboration of the National Strategy must also be considered in the context of the government's efforts to promote electronic governance. As in other OECD countries, the increasing importance of e-government is believed to act as a powerful driver for information security policy, since only reliable and trusted activities can be carried out online.

The Norwegian authorities have been actively promoting e-government for several years as a means to improve the quality and efficiency of public sector activities and services. Five e-government planning documents have been elaborated since 2000: eNorge 1.0, 2.0, 3.0; eNorge 2005 (Norwegian Ministry of Trade and Industry, 2002); and eNorge 2009 (Norwegian Ministry of Modernisation, 2005). The latest plan focusses on the societal potential of IT. One of its salient features is to set targets regarding access to the Internet and IT knowledge and capability in the general population. For government services, it is planned that all interactive services that outreach to citizens become accessible through the citizen portal MyPage (MinSide)[2] For services with a great user volume (taxes, higher education enrolments), the objective is to have at least 75 percent of the target group using the electronic services in 2009. The public sector will also increasingly use open

[2] MinSide was launched at the end of 2005 with services related to property and taxes, health services, education services, etc. www.norge.no/minside

standards and open source code (all new IT and information systems in the public sector are concerned by 2009).

1.1.2. Objectives and orientations

The National Strategy for Information Security was adopted in July 2003, with three ultimate goals: reducing vulnerabilities related to information systems and networks; promoting a culture of information security;[3] and facilitating electronic commerce. To this end, the Strategy contains a series of strategic orientations (Norwegian Ministry of Defence, Ministry of Trade and Industry, Ministry of Justice and the Police, 2003):

- Adequate protection of critical IT-infrastructures.
- Co-ordinated development and enforcement of information 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, based on self-regulation and, if necessary, government 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 levels of education in information security.

[3] 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.

- Creation of a national infrastructure for electronic identification and electronic signatures.

- Active participation in international arenas for co-operation on information security.

1.1.3. Major roles and responsibilities inside the government

The implementation of the Strategy and other parallel policy measures have produced an extensive body of laws and regulations directly or indirectly related to information security, as well as a new government organisation for information security management.[4]

The Ministry of Defence is responsible for managing the Act relating to Protective Security Services, applicable to both central and local government as well as to some other specifically mentioned enterprises. Each individual sector authority has responsibility for ensuring preventive security according to the Act.

The Ministry of Justice and the Police has overall responsibility for national security in peacetime, including a co-ordination role with regard to the protection of critical information networks and systems. The Directorate for Civil Protection and Emergency Planning (DSB), the technical arm of the ministry, has a department dedicated to national preparedness planning which elaborates preparedness plans and risk and vulnerability assessments.

The National Security Authority (NSM) co-ordinates preventive information security measures and verifies 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. The NSM also collects and evaluates relevant information, develops technical and administrative security measures, issues regular threat evaluations and vulnerability reports, and gives advice. The NSM was established on 1 January 2003 and is funded and managed by the Ministry of Defence. It reports to the Ministry of Defence on military issues and the Ministry of Justice on civil issues.

[4] The Norwegian authorities in charge of information security are described in Annex 4 according to their function, following the review’s methodology for analysing risk management systems.

The Warning System for Digital Infrastructures (VDI), a network of major private and public infrastructure operators and intelligence authorities (public-private partnerships) is a branch of the NSM.

The NSM also hosts the main national CERT (Computer Emergency Response Team), NorCERT, which was launched in 2004 as a project and selected in 2005 to become the centre of co-ordination of response to cyber attacks on critical infrastructures in both the public and private sectors.

The NSM also hosts SERTIT, the Norwegian certification authority for information security, responsible for operating the certification scheme concerning IT products and systems. The standard used is ISO/IEC 15408, similar to Common Criteria version 2.1.

Norsk Accreditation is responsible for the certification of organisations' information security management performance in accordance with ISO/IEC 17799.

The Ministry of Modernisation co-ordinates information security for non-classified information and systems and is responsible for co-ordinating national IT policy, including information security. Co-ordination of the work on information security consists of: identifying and following up cross-sector issues and implementing and/or co-ordinating horizontal measures; developing cross-sector strategies and policies on information security and providing them to cabinet for decision; participating in relevant international forums and safeguarding Norwegian interests there.

The Ministry of Transport and Communications has the responsibility for a secure Internet.

The Norwegian Post and Telecommunications Authority (NPT) is an autonomous administrative agency under the Norwegian Ministry of Transport and Communications. The NPT is the principal monitoring and regulatory agency in the field of postal and telecommunications services in Norway, in charge of the enforcement of the Act on electronic communications.

A Centre for Information Security (SIS) was established in 2002 on a three-year trial basis and placed under the jurisdiction of the Ministry of Modernisation. The SIS is a public-private partnership, and mainly deals with awareness-raising among public and private actors. During its trial phase, SIS was connected to a university sector CERT, UNINETT CERT, located in Trondheim. In 2005, it was decided to make SIS a permanent organisation, and to move it from Trondheim to Gjøvik, which is a regional centre for IT expertise and business development. In its new location, SIS will focus on information-sharing and awareness-raising, with SMEs as its main target group.

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 government information security policies. The Council, chaired by the Ministry of Modernisation, consists of representatives from seven ministries, the Prime Minister's office and nine different directorates. The NSM acts as its secretariat. The Council's mandate is to co-ordinate the future evolution of the legislative framework regarding information security, to develop common standards and working methods for information security, and to co-ordinate control activities. The Council is also in charge of discussing broader issues related to risk and vulnerability, and contributes to improved information activities and preparedness planning. The Council also keeps track of the strategic orientations presented in the National Strategy for Information Security, and ensures that all responsible authorities participate.

In summary, the Norwegian government's organisation for information security management is characterised by the sharing of roles and responsibilities among several ministries with their related agencies, and in addition several newly-created entities with diverse affiliations. This organisation conforms to some of the fundamental principles of the Norwegian political system (see box 1.1).

1.2. Policy analysis

The analysis presented in this section refers to both the National Strategy for Information Security and the way it is being implemented by the Norwegian government.

Box 1.1. Aspects of the Norwegian political system

Two important features of the Norwegian political system are of particular relevance when examining information security management.

The first of these is the principle of sector responsibility, according to which the political head of a ministry is directly responsible for all actions of the ministry in relation to the Storting, Norway’s parliament. The minister can be personally impeached by the Parliament before the Court of Impeachment. This principle is embedded in the Constitution (§§ 5 and 30).

The second (related) point is the highly decentralised structure of the Norwegian government. This applies to relations between central and local government (433 municipalities, 19 regions), which enjoys a relatively high degree of autonomy. But it also applies within the central government itself, where Norway has a tradition of small ministries and autonomous and semi-independent technical agencies. Technical expertise and strategic capacity tend to be concentrated in the agencies.

In addition, emergency preparedness and management in Norway is based upon the principles of responsibility, proximity and equality, in the area of information security as elsewhere.

- The principle of *responsibility* states that in public as well as in private activities, responsibilities should be the same whether dealing with a normal or an unusual situation. For instance, each ministry is responsible for emergency planning within its own sector. In addition, the principle holds each citizen responsible for his or her own safety.

- The principle of *proximity* states that crisis management should be handled at the lowest possible level.

- The principle of *equality* states that society at large must be able to operate in accordance with normal standards no matter what challenges it is exposed to, and that the structures of responsibility be maintained in unusual situations.

1.2.1. Scope and objectives

With the Strategy, Norway's government has adopted a broad, ambitious approach to information security. The strategic orientations listed in the previous section cover a large number of aspects of information security management. The actual implementation of the Strategy, however, does not always seem balanced in its approach to the various aspects of security.

Information security encompasses three fundamental properties of an information system or network:

1. Confidentiality, i.e., a computer system or network's ability to store sensitive information in a secure manner and to restrict access to designated users.
2. Integrity, i.e., the assurance that programmes and data are designed and modified only in an authorised manner, and hence are reliable.
3. Availability, i.e., continuous accessibility and service of the computer system or network to users without delays or blackouts.

The relative importance of the three aspects of security varies according to the circumstances and the type of activity supported by the affected system. For issues of national security, confidentiality is traditionally considered the most important. By contrast, the continuity of economic activity – including that of the government – primarily depends on availability. Any systematic bias in the approach to confidentiality, integrity and availability amounts to favouring the reduction of a certain type of risk at the expense of others.

From a legal standpoint, the current legislation emphasises confidentiality (classified information, privacy protection), while paying less attention to integrity and availability. The Act Relating to Protective Security Services, in particular, is focussed on the protection of (confidentiality of) classified information, and does not play a significant role in the protection of unclassified information, which can be of equal importance. The legislative developments under consideration when this review was conducted did not seem to address this tendency adequately. The imbalance in the Act regarding confidentiality, integrity and availability probably stems from the fact that a number of sector regulations include provisions on the two latter aspects. This is the case, for instance, with the Act on electronic communications and the rules applicable to financial institutions (see box 1.2). However, each of these regulations concerns only a fraction of the country's critical infrastructures. There does not seem to be a significant effort to co-ordinate these sectoral approaches, or to define a "security baseline" across sectors.

Box 1.2. Examples of sector specific regulations regarding information security

Electronic communications

The Act on electronic communications (Lov om elektronisk kommunikasjon), effective since 2003, contains several provisions related to information security. In particular, providers are obliged to offer electronic communications networks and services with the necessary security for users in time of peace, crisis and war. Furthermore, the providers shall maintain the necessary levels of preparedness and give priority to entities of importance to society when necessary.

The type and nature of security and preparedness measures are not explicitly laid down in the regulation, but are subject to the principle of due diligence. This will normally include activities such as the creation and maintenance of contingency and preparedness plans, participation in exercises, physical protection of installations, etc. The costs will in principle be covered by the operators themselves. However, if the providers can document that the costs engendered by security and preparedness measures exceed the cost of a purely commercial operation, the government will reimburse the additional cost.

The Norwegian Post and Telecommunications Authority is responsible for enforcing the Act. This entails supervision and audits, where cooperation and provision of information is mandatory for all providers (including security-classified information); and issuing directives of rectification, penalties, revocation of granted permissions, and ultimately closure of operations.

Financial institutions

Requirements for information security for financial institutions are laid down in the "Regulations on the Use of Information and Communication Technology" (IKT-forskriften), introduced in 2003.

According to these regulations, the organisations concerned have to carry out risk analyses at least once a year, or when modifications occur which may "significantly" affect information security. Furthermore, the institutions must have an updated continuity plan and a disaster recovery plan. All these measures must be documented.

The Norwegian Financial Supervisory Authority is mandated to carry out information security audits in the institutions covered by the legislation, through a combination of surveys and physical audits. The audit is process-based and relies largely on the CobiT (Control Objectives for Information and Related Technology) framework, which is issued by the IT Governance Institute and applied by the European Union, among others.

The Authority may also choose to carry out interviews in order to inform itself about current practices in the sector. In 2004, information security audits were carried out in 18 financial institutions, and key personnel in 12 central institutions were interviewed about selected topics (e.g., personnel, confidentiality, integrity and availability, IT infrastructure, process management).

The Authority carries out an annual risk and vulnerability assessment at national level using the results of the audits and interviews, in addition to information security events, international developments and risk and vulnerability assessments. The assessment focuses on identifying elements of risk and possible measures of response. The first assessment was carried out in 2002.

Source: Norwegian Financial Supervisory Authority

From an institutional standpoint, the National Security Authority (NSM) appears to be a key actor in the implementation of the Strategy in terms of both advice and audit: its tasks include approving systems used to protect confidential classified information, setting standards and guidelines, and performing system audits. The NSM is in a unique position between the military and the civil sectors, with supervision on questions of physical and personal security in addition to information security. It should be emphasised, however, that the NSM is exclusively funded by the Ministry of Defence. Its scope is limited to classified information, while sector competencies remain essentially in the domain of each ministerial department.

The major shortcoming of the current approach is therefore to leave a gap, both legally and in responsibility, regarding the protection of valuable unclassified information and assets.

1.2.2. Controls and responsibilities

As a result of the focus on confidentiality, the control processes for non-classified systems are incomplete. The Ministry of Modernisation has responsibility for co-ordinating information security for non-classified information and systems. However, the role of co-ordination seems to carry little authority, and the actual role of the Ministry seems constrained by the willingness of the other ministries to co-operate with its initiatives.

The National Information Security Coordination Council (KIS) appears to be halfway between two role models. According to its official mandate (and name), it should be the principal co-ordinator of government policies, but it has not been vested with the authority to fulfil such a mission. Through its actual capacities and mode of operation, it could be an open forum for discussing and improving government policies. However, the KIS might not be open enough to non-government actors to play that role effectively. Under the present governance structure, there is a risk that some public or private actors perceive the KIS as an extension of the intelligence and law enforcement authorities.

1.2.3. Roadmap and feedback

The Norwegian government has developed a number of important policy tools in order to implement the National Strategy for Information Security, in particular the VDI, NorCERT, the SIS and the KIS. Most new structures are initially launched as pilot projects, tested and only made permanent later. The same approach applies to laws: the Act Relating to Protective Security Services, for instance, is currently being amended and completed. As explained earlier, this gradual approach seems to be well-adapted to the novelty of information security as a field of policy and to the speed of change in technology, applications, and risks.

A general reappraisal and renewal of the National Strategy is planned for 2006, based on experience gained and additional analyses, under the aegis of the KIS. The KIS secretariat follows up the implementation of the various measures by each ministry or agency, and at regular intervals disseminates a progress report to all KIS members. The objective of this follow-up is to give the KIS members a common view over the process of implementation, and to identify areas where further co-ordination needs to be discussed.

This process of monitoring and feedback seems to have two major limitations. First, it does not explicitly link the proposed measures with the strategic orientations, and hence does not identify gaps between the implementation and the final objectives of the Strategy. There is no way of measuring the extent to which the proposed measures, even if correctly implemented, help to attain the goals of the Strategy. In addition, there is no indicator of the quality of implementation of the measures, and the KIS has no investigation capacity. Second, it is not clear how corrective measures would be taken if necessary, in order to feed a continuous process of learning and renewal, since the topics of work of the KIS have to be defined by consensus.

One useful example in this respect is the US Federal Information Security Management Act of 2002, which explicitly addresses control and effectiveness issues. The Act requires federal agency programme officials, Chief Information Officers and Inspectors General to conduct an annual review of their agency's security programme and report the results to the US Office of Management and Budget, which then informs Congress about progress through yearly reports. In addition, the US General Accounting Office has identified federal information security as an area of priority, and actively monitors the implementation of the US Strategy to Secure Cyberspace at both the agency and government department level.

1.3. Conclusion and recommendations

Findings

The review of the National Strategy for Information Security and its implementation shows a number of strong points and some opportunities for improvement. With regard to its scope and objectives, the Strategy outwardly covers the broad spectrum of information security management issues, stating in particular that "critical IT infrastructures shall be protected in terms of availability, integrity and confidentiality." When it comes to the actual tools of security policy, however, the availability and integrity of information are highly dependent on sectoral approaches. At the cross-sector level, the approach seems focussed on protecting the confidentiality of classified information, and the emphasis on defining a baseline in terms of availability and integrity is less than adequate. The co-ordination and control mechanisms in place exhibit the same tendency, as the entities in charge of co-ordinating security measures for non-classified information do not seem to have the necessary authority to fulfil all of their formal responsibilities. While the implementation of the Strategy follows a learning approach and is well-adapted to the reality of information security management, there are opportunities to strengthen the monitoring, feedback and appraisal of implementation measures.

Opportunities for action

- The policy options for sharpening the focus on availability and integrity include redressing the imbalance among security, availability and integrity in the Act Relating to Protective Security Services in the new legislation currently under consideration regarding the protection of objects and assets. This would entail extending the scope of the Act from classified information and systems to include information and systems of relevance to the nation's security and societal welfare (e.g., critical infrastructures).

- Responsibility assignment could be improved regarding the management of non-classified information, in particular in areas such as the co-ordination of ministerial initiatives, the provision of standards and guidelines for "fault tolerant" systems, and backup and disaster recovery procedures. These could be set at a general level as part of promoting the concept of a baseline of minimum national preparedness (this issue is addressed in more detail in Recommendation 5).

- The role of civil actors in developing information security policies could be strengthened. The knowledge and expertise of a broad range of actors from both military/law enforcement and civil sectors is needed in order to clarify concepts such as "critical infrastructures", "societal security" and "continuity of supply"; and to organise risk management activities accordingly (see also Recommendation 6).

- The learning approach to the implementation or improvement of the Strategy could be enhanced by setting detailed objectives for each ministry, measuring progress towards these objectives, and appraising the overall performance of the information security management system in the prevailing risk situation on a regular basis.

Recommendation 1: Develop the appropriate tools and improve the sharing of responsibilities for information security policy in order to better address availability and integrity needs.

Recommendation 2: Elaborate a performance appraisal process to measure the effectiveness of current information security control processes against current threats.

Chapter 2. Assessing Information Security Risks

The aim of risk assessment is to complete a systematic analysis of the security requirements for a particular system or network in order to maintain its confidentiality, integrity and availability. For this, risk assessment comprises a step-by-step evaluation of the components of risk, namely the probability of occurrence of a harmful event and its consequences:[5]

- The assets inside the system or network are identified, and their relevance for the overall functioning of the system is evaluated.
- The value of identified assets is estimated, and an impact is associated with the loss of confidentiality, integrity or availability.
- Significant threats and vulnerabilities are identified for each asset.
- The likelihood of the threats and vulnerabilities occurring is estimated.
- Risk is calculated as the combination of (when possible, the product between) the probability of occurrence of a harmful event and its consequences.
- Risk might, in addition, be evaluated against a predefined scale.

In the area of information security, risk assessment is generally seen as a necessary first step of any risk management procedure[6] – this is, for instance, what international standards of information security management such as ISO 17799 require. The OECD Guidelines for the Security of Information Systems and Networks emphasise the need not only to conduct risk assessments (Principle 6), but also to reassess the security of information systems and networks on a regular basis (Principle 9), (OECD, 2002).

The owners and operators of information systems and networks are generally best placed to conduct risk assessments, not least because they have better access to system-specific information. For an external actor, the

[5] One example of a risk assessment methodology is EBIOS (see Grall (2005), and EBIOS (2004), on the SGDN website www.ssi.gouv.fr/en/confidence/ebiospresentation.html).

[6] The overall risk management process is defined in ISO Guide 73 (2002).

difficulties of collecting such information across organisations are almost insurmountable. It is for this reason in particular that available estimations of the impact of information security failures are not reliable (see box 2.1).

Hence, the first task for government is to conduct risk assessments concerning its own information systems and networks.

Box 2.1. – Evaluating the costs of information security failures

Evaluating the costs of information security failures poses a number of methodological challenges, such as 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; and how to account for indirect costs such as security expenses (e.g., the overhead costs of an incident response team). There is no standard, widely accepted method for dealing with these questions. [1]

Because of the scarcity of information and the lack of a consistent cost assessment method, estimates of the economic impact of information security failures are commonly based on surveys among organisations. For instance, a global survey conducted in 2003 by PriceWaterhouseCooper among 1000 companies in 50 countries found that their average loss caused by malicious acts amounted to USD 0.8 million in the two previous years. The US-based Computer Security Institute runs an annual survey with the help of the FBI, and finds results on the same order of magnitude (USD 0.5 million average loss in 2003, following 0.8 million in 2002)[2]. However, such results cannot be interpreted as accurate measures of the costs of information security failures 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 in the first survey and half the participants in the second were unwilling or unable to quantify their losses. In addition, as the survey samples do not aim to be representative, the results cannot be extrapolated rigorously to national or global level. In the case of the US survey, the sample changes every year, which makes it difficult to analyse evolutions from one year to the next.

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 price falls substantially (on average by about 2%) relative to the market.[3] 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 evaluated objectively. 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.[4] 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 sums quoted are astronomical: USD 225 to 275 billion in 2003, and USD 186 to 228 billion between January and March 2004.[5]

A range of evaluations which largely differ in their approach, scope, methodology, and, not surprisingly, in their results is available. For instance, the cost estimates of damage due to the 2003 computer worm SoBig (reported in the media) went from USD 1 billion to USD 31 billion (Congressional Research Service, 2004, p.12). 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 doubled (according to CSI/FBI data), quadrupled (according to CEI), or went up a hundredfold (Mi2g)" (ibid. p.11). Depending on the source, the worst year in terms of loss is 2000 (CEI), 2002 (CSI/FBI), or 2004 (Mi2g) (ibid. pp. 9-12).

Notes:

[1] For a discussion, see Soo Hoo (2000), chapter 3.

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

[3] 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 (2004), *The Economic Impact of Cyber Attacks*.

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

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

There are in addition areas where government has a role in risk assessment beyond its own sphere of operation, in order to account for the "externalities" of information security. Externalities are the costs or benefits of a private agent's actions for the rest of society, which justify that society as a whole gives more value to these actions than the private agent does. In information security, externalities are an important feature of networks, since all participants in the network benefit from increased security in a particular system (equivalently, all participants are affected by a security failure in a particular system). Chapter 3 further develops this question.

Archetypical examples of externalities are the so-called "critical information infrastructures", where an information security failure can lead to the disruption of one of society's "lifelines" (health, power supply, etc.) and generate considerable direct and indirect costs for other actors (as described in box 2.1). Critical information infrastructure systems support the continuity of supply in a country in many ways. A simple example is supply chain automation linked to just-in-time delivery, making IT systems critical to the continuity of supply of essential goods or services. In extreme cases, failure of an IT system can lead to the whole chain of supply being crippled.

In order to lead to appropriate decisions with regard to security management, risk assessments need to integrate such spillover effects. The role of the government in this regard can be to gather information on external costs and benefits, or on interdependencies among critical infrastructures; to provide that information to a system's owner/operator; and more generally, to ensure that risks are appropriately assessed from the standpoint of society as a whole.

The role of government with regard to the assessment of risks to information security can be summarised as:

- To assess risks concerning its own operations.

- To ensure that a comprehensive and consistent assessment of risks is conducted on behalf of society as a whole, in order to identify the nation's critical information infrastructures and evaluate their security requirements; and to ensure that the assessment is updated periodically.

2.1. Risk assessment in the government

2.1.1. Statement of the issue

The greatest challenge in assessing risks in government information systems is the complexity of the government as an organisation.

The issue of complexity starts with defining what has to be protected, or in other words, in setting the security boundaries. This is the first step of security management, as these boundaries will also define who should have authority and responsibility for security. In this regard, information security is similar to physical security, except that the boundaries are more often logical or virtual – although they can still be combined with physical ones, as in the case of separation of encrypted and plaintext data on a cryptography microchip (so-called “red/black” signals).

Once the IT assets (physical or digital) have been defined with their boundaries (physical or logical or virtual), the next step is to perform a classic risk assessment. This can be a challenge in a complex organisation where responsibility for some IT systems and services crosses organisational boundaries. In some cases, it might be possible to define organisational responsibilities in terms of security boundaries, then to use this method to identify the interfaces, and so break down a complex security situation into a number of simpler, more manageable ones where a detailed risk analysis is practical. However, in the case of multiple services supported by complex IT systems and networks, such breaking down is often impossible.

Sophisticated tools have been developed for assessing risks inside complex systems. One method is based on root cause analysis, where each separate process or activity is modelled in detail and then a risk assessment is conducted for each stage. This method is often used by banks to assess the security of their transaction processes. Implementation of root cause analysis usually requires knowledge and, ideally, ownership and control of the end-to-end processes. This makes it unsuitable for some environments, including that of governments.

The most common approach to dealing with complexity is to establish a general security baseline, and exceptionally perform a detailed risk analysis only for specific cases. The baseline is a combination of measures based on technological standards, management processes and operator procedures following best practice. It has to be tailored to the organisation’s environment, and determined on the basis of an assessment of the general level of risk. It is usually estimated that in order to be tractable, baselines should be designed to address up to 80 percent of the organisation’s information security requirements. The remaining 20 percent of information security requirements can then be identified in screening processes where sector managers review their activity against its specific risks, and decide whether the information security baseline satisfies their requirements or not. In a minority of cases, a detailed risk assessment then needs to be performed.

This type of approach has become widespread in industry and government sectors with the publication of international standards such as ISO 17799. Because it establishes a basis for comparability, it enhances trust. For instance, in public/private partnerships such as the health sector, demonstrable adherence to an information security baseline can create the necessary level of confidence for the exchange of sensitive medical and personal information that enables the whole system to function. Another merit of the approach is to establish information security management processes that are consistent with other management control processes, and can be easily embedded into existing practices.

However, effectiveness crucially depends on the setting and enforcement of central organisational standards for the protection of information. Exceptions in this regard need to be as few as possible, since each of them creates the need for a detailed risk assessment, and also erodes the common baseline.

2.1.2. Policy analysis

Norway, like other countries, has adopted ISO 17799 as the standard for security management, and put in place a national accreditation scheme for it. However, there is no process to drive the implementation downwards and embed it into government business processes. In the first place, there is no explicit government requirement to demonstrate compliance with the standard by voluntary self-declaration or formal certified accreditation. In addition, it has to be emphasised that security management standards have to be implemented on the basis of each organisation's specific security technology, management processes, and operational procedures. Chapter 4 addresses the question of establishment, implementation and enforcement of standards in detail.

One of NSM's missions is to promote risk assessment in government systems. For this, the Agency has developed a risk and vulnerability assessment methodology for classified information systems, and also publishes annual risk assessment reports. However, there is no systematic process of risk assessment in the government, and risk assessments are not used as a complement to a baseline approach to security.

2.1.3. Conclusion and recommendations

Findings

Risk assessment regarding government systems is incomplete. A general standard has been adopted for the government, but is not implemented as a security baseline, and therefore cannot help to simplify the challenging task of assessing risks to government systems.

In the absence of a complete and consistent assessment of risks, it is difficult to assign comprehensive responsibility for security management, and set priorities for government action.

Opportunities for action

- Norway could initiate a project to implement an information security management standard such as ISO 17799 as a security baseline in all government IT-related activities. Based on the experience of other governments and large organisations, a gradual process of implementation could be defined: Norwegian ministries could for instance aim to achieve self-declared compliance with the standard within five years; then a formal certification in the Norwegian accreditation scheme would be requested within ten years. Such a systematic approach would have the advantage of setting an example for the private sector.

- In addition, Norwegian internal and third party IT contracts could contain a requirement for demonstrated compliance with relevant information security standards and guidelines. Norwegian internal and third party network connection agreements could also contain a requirement for demonstrated compliance with relevant information security standards and guidelines.

- The NSM could provide Common Criteria Protection Profiles for certified products and systems that are also consistent with information security management defined by ISO 17799 to meet the requirements of the Act Relating to Protective Security Services.

- A ministerial level risk assessment could detail security requirements and clarify the rules of the game for implementing a security management standard as a baseline. Some of these requirements could be defined by compliance with general government security laws, data protection laws and the like. Others could aim at ensuring continuity of supply of essential services in the ministry's sector.

Recommendation 3: Define and implement a baseline approach to security management in government systems, complemented by focussed risk assessments.

2.2. Risk assessment in critical infrastructures

2.2.1. Statement of the issue

The assessment of risks from a societal point of view entails measuring the potential impact of information security failures on national security and societal welfare. The first step for this is to define the latter notions in terms of the continuity of supply of vital services, government operations (including e-government) and private sector operations (including e-business) – in other words, to identify the nation's critical infrastructures. The second step is to evaluate the dependence of each of these infrastructures on reliable information systems and networks, and their exposure to threats. The final step is to determine if the resulting risks to societal welfare and national security are acceptable.

This process comprises a host of challenges for governments. To mention but a few: to build a consistent approach across all sectors of activity, whether these are predominantly market-based or not, private or public; to define priorities among assets, for instance among those deemed "critical" and those which are only "important"; to clarify the conditions under which decision support tools such as cost-benefit analysis can be used;[7] to evaluate interdependencies and cascading effects among infrastructures; and last but not least, to overcome political difficulties in order to build a consensus on the design and outcome of the process.

However, several OECD countries have launched initiatives to identify critical infrastructures and assess the related risks in recent years (see box 2.2), and their experience yields a number of interesting lessons.

First, identification methods may differ widely according to particular national concerns and experience of accidents involving critical infrastructures. Second, the number and nature of critical infrastructures identified is also different from country to country, although communication, energy, transportation and finance are included by all countries (see table 2.1). Indeed, the definition of a critical infrastructure may depend on the specific structure of the national economy, e.g., surface water management in the Netherlands is a critical infrastructure, as are nuclear power plants in France. What seems important is that the identification of critical infrastructures is the outcome of a dialogue among all the relevant stakeholders.

[7] See for instance National Research Council (2003), p. 64; and ISAC Council (2004a), p. 2.

Box 2.2. The identification of critical infrastructures in some OECD member countries

Critical infrastructure protection has received considerable attention in OECD member countries in the past decade. The most widespread initiatives have consisted in identifying national critical infrastructures, as a first step to risk assessment and protection. Countries that have carried out activities in this field include Canada, the Netherlands and Germany.

Canada and its Quebec province initiated work on critical infrastructure interdependencies after the ice storm that hit Canada and the United States in January 1998, and which lasted for seven days. It led in particular to severe interruptions to electric power supply in Canada, destroying 120 000 km of power lines and telephone cables, 130 major transmission towers and 30 000 wooden utility poles, with dramatic knock-on effects on water supply. Electricity supplies to 3 million people were cut, and in some areas it took three and a half weeks to restore power.

The Netherlands has established a detailed mapping of its critical infrastructures and their interdependencies, in close cooperation with the private sector.

Germany has developed a specific methodology aimed at better analysing and understanding critical processes at a relatively detailed business level. The main line of argument is that business processes that are vital for the continued existence of an enterprise are "business-critical". If the existence of an enterprise is vital for the functioning of a sector, the business process also becomes "sector-critical", although this is generally restricted to oligopoly situations (i.e., only a few market actors). It is assumed that society-critical and sector-critical processes coincide.

Sources: Quebec Ministry of Public Security (1999); Netherlands Ministry of the Interior and Kingdom Relations (2003); BSI (2004).

Table 2.1. Mapping of critical infrastructures in selected countries

	AUS	AUT	CAN	FIN	FR	GER	IT	NL	SWE	CH	UK	USA
Communications	X	X	X	X	X	X	X	X	X	X	X	X
Energy	X	X	X	X	X	X	X	X	X	X	X	X
Emergency services*	X	X	X	X		X	X			X	X	X
Finance	X	X	X	X	X	X	X	X	X	X	X	X
Food supply	X		X	X		X		X			X	X
Government services*	X	X	X	X		X	X		X[1]		X	
Health	X	X	X	X	X	X	X	X		X	X	X
Higher education												X
IT		X	X	X		X	X[2]					X
Legal order								X				X
Manufacturing	X		X	X[3]	X[4]					X		X[5]
National icons	X		X									X
Nuclear power stations					X							X
Public administration*										X	X	
Public safety and order					X			X			X	
Social welfare		X		X								
Surface water management								X				
Transport	X	X	X	X	X	X	X	X	X[6]	X	X	X
Utilities (water and waste management)	X	X	X	X	X	X	X	X		X	X	X

* The definition of these services may vary from country to country.

[1] National command systems
[2] E-government
[3] Defence-related
[4] Chemical and biotech
[5] Defence industrial base
[6] Air traffic control systems

Source: Comprehensive Risk Analysis and Management Network (2004), *International CIIP Handbook 2004*, Center for Security Studies, Swiss Federal Institute of Technology, Zurich.

2.2.2. Policy analysis

In Norway, the identification of assets relevant to national critical infrastructures and the practice of risk assessments seems to be a work in progress. While the National Strategy for Information Security clearly gives directions to protect national critical infrastructures (see next chapter), it is less clear about what is considered to be within the scope of "national security". There do not appear to be explicit links between "national security", "critical infrastructure protection", "societal security" and "continuity of supply". Nor is it clear what each actor understands by these terms.

Several lists of critical infrastructure sectors have been established in the past (e.g., in the report "A Vulnerable Society"). The topic of societal vulnerability has been the subject of a series of vulnerability studies carried out by the Norwegian Defence Research Establishment (FFI) since 1994 within the framework of the BAS (Beskyttelse Av Samfunnet – protection of society) projects. Some sector-wide studies have been carried out in telecommunications, transportation, energy supply, and water supply. One cross-sector study has also been carried out. However, none of these reports considers information assets and security as such.

In addition, public services that might qualify as critical infrastructures do not seem to be identified systematically.

Concerning the practice of risk assessment, NSM has a mission to make standard tools available to operators, give advice on their use, and possibly to audit risk assessment procedures, wherever classified information is involved. However, beyond this mandate regarding classified information, no one has responsibility for overall supervision of the practice of risk assessment in various ministerial departments and critical infrastructure sectors. The principle of sector responsibility applies here, with substantial differences among sectors due to specific regulations. The telecom regulatory agency NPT, for instance, can perform risk assessment in the telecom sector and check risk assessments carried out by private operators, in application of the Act on electronic communications. But a similar degree of regulatory control does not seem to exist in other sectors (e.g., power generation).

As a result, Norway does not seem to have a sufficient overview of possible risks for information security in interdependent critical infrastructures.

This, however, may be changing. The broadening of the scope of the Act Relating to Protective Security Services from classified information to "vital objects" is a first step, although it is still limited to systems supporting classified information. A new project has been launched in the BAS series to map and assess the dependence of critical infrastructures on IT. The BAS5 project could make an important contribution to investigating Norway's IT-related vulnerability – provided it is elaborated in closer interaction with the operators (both public and private), with a view to their conditions of operation (see Recommendation 13). A government commission was established in 2004 to make an inventory of critical infrastructures in Norway (whether public or private), with the following mandate:

- Identify activities that ensure the interests of national security and other interests that are considered vital to the nation, in other words identify critical infrastructures.
- Identify and assess measures to protect critical infrastructures.
- Assess all activities responsible for critical infrastructure, particularly those that are not publicly owned or operated.
- Assess which infrastructures the government should own completely or partially.
- Consider the administrative and financial consequences of the proposals.

The findings of the commission were not available when finalising this report.

2.2.3. Conclusion and recommendations

Findings

Risk assessment regarding critical information infrastructures is incomplete, but the BAS5 project and especially the work of the Government Commission on Critical Infrastructures might provide a solid basis for it.

Opportunities for action

- As a follow-up to the work of the Commission on Critical Infrastructures, a process of dialogue involving the users, suppliers and regulators of critical infrastructures could be developed across sectors, in order to clarify issues of risk assessment, in particular with regard to information security (see also Recommendation 6).

- The opportunity could also be offered to users and suppliers of critical infrastructures to make inputs to the BAS5 project (see also Recommendation 13).

Recommendation 4: Put in place a systematic process of risk assessment for critical infrastructures.

Chapter 3. Protecting Information Systems

The arguments put forward in Chapter 2 to delimit the role of governments in risk assessment are also valid when it comes to protecting specific information systems. This defines two major areas of government responsibility:

1. As for any owner or operator, the government has to protect its information systems and the processes that they support.

2. In order to safeguard national security and social welfare, the government has to ensure that critical infrastructures are adequately protected.

When reviewing the policy measures to implement the OECD Guidelines for the Security of Information Systems and Networks, the OECD Secretariat has identified two major drivers of information security in the Member Countries: the security implications of e-governance, and the protection of critical infrastructures (OECD, 2004a).

3.1. Protection of government systems

3.1.1. Statement of the issue

Government dependence on IT systems and infrastructures is increasing, and already hardly any system could fully function without IT. This is not an entirely new situation, as government finance systems, for instance, have been relying on IT applications for many years. What has changed in recent years is the pace and degree of dependence, which has extended to even minor functions within government. With the implementation of modernisation and e-governance plans in public administrations, a large number of government services have become accessible through information networks.

The most significant example of this is related to data protection and the identity of citizens within government IT systems. Instances of identity theft and social welfare payment fraud have increased to the point where stronger protection of the electronic identity of the citizen has become essential for effective government. While it is not economically viable to create and maintain separate identities for each citizen in every government IT system, the use of national identity cards that carry the details of the individual citizen electronically is inevitable in important electronic government applications. For instance, electronic passports are increasingly widespread in OECD countries. All this is creating a heightened sensitivity to the security and protection of government IT systems and infrastructures in the wider population, and most countries now have data protection and privacy regulations and laws in one form or another.

The ubiquity of IT applications and the increasing importance of data protection impose higher requirements on government systems of protection against IT threats and incidents. To achieve this, a minimum level of co-ordination across government agencies is necessary in all aspects of government IT usage. The absence of co-ordination with regard to IT usage carries with it a number of costs, due for instance to redundant initiatives or lack of interoperability. However, the main problem of a non-co-ordinated approach is the possible security gaps that occur when sectors are individually responsible for their information security, while at the same time having unequal access to IT expertise and resources.

The Norwegian health sector can be taken as an example: the sector has just created a nation-wide network where users are responsible for the security of their individual information. Ideally, the health services network would be an open network among subscribers. However, this would expose individual users to security lapses caused by other users on the network. To avoid this, the network is, at present, a number of fragmented security "islands" connected by communications networks. This has created a number of security barriers to the flows of health care information, undermining some of the information-sharing reasons for creating the network in the first place.

3.1.2. Policy analysis

It is important to note, however, that a high degree of co-ordination does not necessarily entail centralised management of government information systems. Indeed, the degree of monitoring of information security policies within the governments of OECD countries is variable. The government of the United States, for instance, has developed a self-assessment tool that all agencies are required to use, and it also requires all government systems to be associated to one security plan, which is accredited and certified before becoming operational (OECD, 2004b, p. 15).

Other OECD countries have elaborated common guidelines, and left it to agencies and ministries to conform to these – these guidelines may be based on international standards, as is the case in the UK or in the Netherlands, or on own standards, as in Germany (OECD, 2005, p. 175).

In a third and final group of OECD countries, ministerial departments have a large degree of autonomy for the security of their information systems. When responsibility for policy implementation is decentralised, a mandate is sometimes given to a government service to verify the actual security of government sites and systems. It should be noted that total decentralisation, i.e., both decentralised policy formulation and policy implementation, is rare – among OECD members, only Italy, Norway and the Slovak Republic have reported having decentralised policy formulation, and Norway is the only country also stressing decentralised implementation (OECD, 2004b, p. 15).

The role of establishing standards is usually delegated to one or two ministries or agencies. In the United States, the National Institute of Standards and Technology (NIST) publishes the Federal Information Processing Standards, which include security standards. Among EU member states, the national standards body is usually mandated for general security, and the national security agency for specifically sensitive information. In the UK, the Department of Trade and Industry also gives advice to other ministries on implementing standards. The Netherlands has a similar organisation, except that responsibility for general government security standards lies within the Ministry of the Interior and Kingdom Relations. In addition, providing advice to national bodies is one of the missions of the European Network and Information Security Agency, ENISA, established in March 2004.

Through these experiences, it appears that a co-ordinated approach is preferable in:

1. Setting security standards, including legislation and regulations.

2. Providing advice on the implementation and operation of the standards.

3. Auditing the operation of the standards.

The assignment of these three areas of responsibility to government actors that are well-identified and have the actual capacity to fulfil their role therefore seems to emerge as a good practice in this area.

In Norway, as explained earlier, responsibility for information security policy is distributed, according to the principle of sector responsibility, and few co-ordination mechanisms exist at the central level. This leads to a number of issues that might affect the general level of protection.

ISO 17799 has been established as a standard and applied in some government organisations. However, as noted in chapter 2, conditions of implementation have not been clarified. During this phase, the standard has to be interpreted in order to fit the specific conditions of each organisation – in other words the ISO 17799 "rules of the game" have to be made explicit for each ministry or sector of activity. The existence of adequate expertise and resources to do so at a decentralised level is open to question. It is also unclear if other agencies with more expertise, such as NSM, have the mandate and resources to assist other government entities in this work.

Regarding audits, piecemeal responsibilities might also leave some gaps: NSM audits only for issues related to classified information, the Data Inspectorate deals specifically with the protection of personal data, and DSB focusses on civil emergency preparedness.[8]

Policy co-ordination is in principle the role of the KIS, a stakeholder panel for all the ministries and agencies involved in information security management, and of the Ministry of Modernisation. None of these two entities has the necessary authority to carry out effective co-ordination.

The KIS has not yet achieved a high degree of co-ordination and control over security in government information systems. Although this might be due to its recent creation, it is questionable whether its present terms of reference and authority enable it to meet its objective. The actual role of KIS is essentially consultative. One of its current activities is to evaluate the existing body of laws and regulations pertaining to information security from a user standpoint, and possibly to propose simplifications. This is an important endeavour, but it is uncertain whether this alone will suffice to give the government a clear view of the effectiveness and shortcomings of the existing legal and regulatory framework. One of the major challenges awaiting the KIS and the government at large in the near future is to achieve the level of overview necessary to identify areas where the National Strategy for Information Security has achieved satisfactory results, and the gaps that are left.

The Ministry of Modernisation's IT Policy Department formally has a leading role in identifying cross-sector issues and co-ordination problems, and in proposing ways forward. However, this role does not seem to be backed by an authoritative decision-making mechanism, and most issues firmly remain under sector responsibility. As a result, the Ministry's actual

[8] It must be noted that the DSB audits on preparedness and contingency planning do not yet cover information security risks. The Agency will hold its first major emergency management exercise concerning an IT crisis early in 2006.

role is practically restricted to emerging issues that do not fall within the scope of another ministry.

3.1.3. Conclusions and Recommendations

Findings

Responsibilities with regard to information security policy are dispersed across too many ministerial stakeholders to be executed consistently.

Opportunities for action

- Norway could consider alternative ways to achieve a more co-ordinated national information security policy. One option could be to assign a clear leadership role to one ministry on all information security issues beyond the present scope of the Act Relating to Protective Security Services, with a mandate to develop information security as an integrated part of e-government and e-business. This could reduce any duplication of initiatives carried out within different ministries and focus efforts on priority issues.

- Another possibility could be to co-ordinate policies regarding information security at cabinet level (as proposed in Recommendation 10 regarding the management of emergencies). Under this model, individual ministries could then take responsibility for the execution of priority actions and delivering the actual improvements.

- An alternative which would be compatible with a decentralised architecture would be to clearly set standards defining the baseline approach at a central level, and monitor and enforce their implementation through management and performance appraisals in the government audit processes.

Recommendation 5: Allocate responsibilities among a smaller number of players inside the government.

3.2. Protection of critical infrastructure systems

3.2.1. Statement of the issue

As explained in chapter 2, government intervention to protect critical infrastructures can be justified by the existence of externalities. Security-enhancing investments undertaken by one participant in a network benefit others through three channels: 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); and third, by ensuring that the organisation's supply of goods and services will not be disrupted following an attack on its information systems, with possible indirect effects on others. Conversely, a participant's lack of consideration for security generates costs for other participants. For an organisation or an individual, increased protection comes at a cost: 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, more complicated procedures, etc.).

The balance between the costs and benefits of security expenditure is therefore less favourable from the standpoint of an individual participant in a network than from that of the network as a whole. 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 undertaken by others, and inadequate overall security limits the development of the network (e.g., communication and commerce on the Internet).

When considering optimal policy design in this area, two major developments from the past two decades are of particular significance.

First, as noted above regarding the government, the ubiquity of IT has led to widespread dependency on IT networks and systems. Nowadays nuclear power plants, air and rail traffic, financial transactions and hospitals are managed through computers and information networks. Computers or computing devices are also increasingly embedded in other appliances, and then networked (National Research Council, 2001). Information systems have become the cornerstone of critical infrastructures, and as a result, the potential damage for society resulting from information security failures has increased dramatically (see box 3.1.).

Box 3.1. Risk related to the increasing reliance of society's critical infrastructures on information systems and networks

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 2002, a British computer administrator was indicted on charges that he had accessed and damaged 98 computers in 14 US states in 2001 and 2002. The networks belonged to the Department of Defense, NASA, and private companies. Allegedly, the attacker had gained administrative privileges on military computers, copied password files and deleted critical system files. The attacks rendered inoperable the network of the Naval Weapons Stations and the Military District of Washington.

In January 2003, the computer worm Slammer 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. The worm also nearly blacked out a 911 calling centre in Seattle; led to the shutdown of Internet service providers in South Korea; disrupted Continental Airlines' schedules as it hit the airline's corporate networks and disabled the ticketing system; 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.

More recently, in 2005 it was reported that the US electric power grid had been the target of hackers and that they had gained access to the utilities' electronic control systems, apparently without causing serious damage. There have also been several incidents of hacks into large databases in universities, compromising personal information of thousands of people at each occasion.

Sources: Poulsen (2003); O'Harrow and Eunjung Cha (2003); Chen (2004); Fisher (2003); US General Accounting Office (2005).

As a result, critical information infrastructure protection is high on the agenda of most OECD countries. One notable example is the US government's National Strategy for Physical Protection of Critical Infrastructure and Key Assets (United States, President, 2003), to which the Strategy to Secure Cyberspace is associated. The latter strategy indicates five priorities, and prescribes detailed actions in each:

1. Developing and enhancing national cyber analysis and warning.

2. Reducing cyberspace threats and vulnerabilities.

3. Promoting awareness of, and training in, security issues.

4. Securing government's cyberspace.

5. Strengthening national security and international cyberspace security co-operation.

The policy implementation of these priorities is an ongoing mission of the Department of Homeland Security, and some aspects of it prove to be challenging.

The second major development in this area is the deregulation and privatisation of formerly state-owned infrastructures, which increasingly operate in a competitive environment. This leads to a shift in the constraints that these companies face, as well as in their objectives and management. As competitive pressures grow, security expenditures will tend to be increasingly considered as an investment that needs to be justified from a profitability standpoint. In addition, the original management and communication lines between government and formerly state-owned utility providers might increasingly be disrupted.

Some of the security implications of this change might not have been adequately anticipated in the new regulatory framework applied to critical infrastructures. This concerns in particular the balance between the level of security that the privatised utility provider might be expected to provide as industry "due diligence" and the level required to meet national security objectives. One aspect of this question is responsibility for the management of interdependencies among infrastructures. As new and competitive providers enter the utilities market, this is an issue that will grow unless it is properly addressed.

Current evolutions in European case law and reflections at EU level can be seen as part of the answer. Building on recent decisions by European courts, the European Commission proposed in a recent draft a number of conditions under which security expenditures could be eligible as public service, thereby justifying compensatory state aid. The conditions principally relate to the clarity of definition of assigned tasks, to the procurement conditions, and to the final impacts on the functioning of markets (European Commission, 2004 and 2005).

3.2.2. Policy Analysis

Norway has made critical infrastructure protection one of the four key targets underpinning information security in society, as expressed in its Information Security Strategy. The Strategy asserts that critical IT infrastructures shall be protected in terms of availability, integrity and confidentiality. In most cases, ensuring availability and integrity will be most crucial. Security measures will need to take into sufficient consideration the maintenance of full system functionality. Enterprises must create their own plans and measures in the event of failures within their own critical infrastructures.

The Strategy includes a number of positive points, in particular the introduction of warning schemes and the widened availability of CERTs (Computer Emergency Response Teams) and ISACs (Information Sharing and Analysis Centres). The government has also stated its intent to use procurement – and therefore the considerable influence that it can have as a purchaser of goods and services – in order to ensure implementation of part of the Strategy.

The Strategy recognises that there will be administrative and financial impacts in implementing the measures, which are to be funded by the ministry in charge within current budget restraints. Private enterprises will normally have to bear costs within their own normal operating costs. However, the Strategy does not identify the triggers (or mechanisms) that will bring government funding into effect. In ministries, calls on budgets for implementation compete with other possible expenditures. In the private sector, as explained, any measure that is likely to affect operating performance or cost is likely to be closely scrutinised with regard to its economic justification. Lack of clarity in the justification or understanding may weaken the business case for budgetary or stronger ties with national authorities.

The sharing of responsibilities between the government and critical infrastructure operators also seems problematic in the existing regulatory framework. Regulatory oversight relationships between sectoral agencies and private operators appear to work well in Norway, including in the use of alternatives to regulation (OECD, 2003b). Regarding information security, however, there are large differences in the degree and nature of monitoring by government agencies across different sectors, with no apparent justification in terms of criticality or vulnerability. In the electricity supply sector, Statnett seems to have a large degree of freedom to ensure the security of its supply. In the telecom sector, by contrast, the Post and Telecom Authority (NPT) is in charge of closely monitoring security in application of the Act on electronic communications.

One particular aspect of the telecom regulatory framework is the financial arrangement between NPT and telecom companies over security spending, according to which expenditures corresponding to specific requirements of the Agency are financed by public subsidies. A recent reform has brought about much-needed improvements in the arrangement: the amount of subsidies is now determined on the basis of projects, and not mechanically carried forward from one year to the other; the scheme has also been extended from Telenor to all telecom operators. The arrangement now seems to respond to some basic requirements of a compensation mechanism for public service, according to which reduction in risk in order to meet specific national critical infrastructure needs can be financed by public funds. However, there remains the challenging issue of determining with enough transparency which level of security a private operator should assure as part of its normal business (industry "due diligence"). The compensation arrangement is also an example of cross-sector differences of approach in the regulation of critical infrastructures that seem to have little justification.

There would therefore seem be a need for a more systematic and transparent approach regarding the sharing of responsibilities in the protection of critical infrastructures, and its financial implications. The evolution in European legislation concerning State aids and public service mentioned above could provide a framework for putting such schemes on a stronger footing.

Finally, co-operation among public and private actors seems to be largely based on informal communication and ad-hoc links, which are likely to become difficult to maintain as market structures increasingly move away from state-controlled monopolies. Operators' involvement in risk management activities also seems to vary considerably, and is too dependent on the regulatory agency and informal networks. While some major operators are involved in information-sharing networks, other important actors are presently overlooked.

3.2.3. Conclusions and recommendations

Findings

Two main challenges in relation to critical infrastructure protection have been identified: first, to clarify the division of responsibilities for critical infrastructure protection between government and operators, including for the handling of interdependencies among infrastructures; and second, to communicate and co-operate with all critical infrastructure owners and operators in a systematic way.

Opportunities for action

- In order to facilitate regular communication and co-operation, the government could carry out a general overview of critical infrastructures actors, large and small, and their security situation (for instance in relation with the BAS5 project).

- A systematic cross-sector dialogue between the government and operators and users of critical infrastructures (as sketched in Recommendation 4) could address the questions of risk acceptability in critical infrastructures, and of the level of security that operators have to ensure as part of their normal business. The output from this dialogue could be a clear allocation of responsibilities among operators, regulators and supervisory bodies regarding Critical Infrastructures Protection (CIP), established in a broader context than regulatory market oversight.

- Various mechanisms could be put in place to ensure that due diligence is respected in critical infrastructures, from liability laws and economic incentives to mandatory audits and benchmarking exercises.

- Responsibilities and authority could additionally be assigned for the management of interdependencies and continuity of supply issues that fall beyond the scope of sector regulators, in co-operation with these.

Recommendation 6: Determine risk acceptability and the sharing of responsibilities in risk management for each critical infrastructure.

Recommendation 7: Strengthen the involvement of operators in risk management activities.

Chapter 4. Managing Incidents, Emergencies and Crises

Information security incidents are common. As they spread and have increasingly severe consequences, they develop into emergencies, and eventually crises (see box 4.1). This escalating process has to be matched by a similar escalation in management responsibilities. As the impact grows, a larger number of actors are concerned and new and unforeseen effects are often triggered. The level of management and response needed to regain control of the situation therefore rises. An important challenge here is to locate the breaking point at which emergency management passes from one phase to the next.

The role of government in alert and rescue interventions follows a similar pattern. Regarding incident response, governments can provide useful support, in particular where local response capacities are inadequate. Government oversight and monitoring need to be stronger in the handling of emergencies through preparedness and contingency planning, especially where critical interests of the nation are at stake. Governments have to take the lead role in the management of crises, in conditions that leave no room for delayed decisions and inadequate effectiveness. The three areas of action mainly consist of:

1. The creation and co-ordination of CERTs, or similar functions, in order to improve incident management, at government, business and SME level.

2. The creation of incentives for preparedness and contingency planning through increased auditing activity and awareness-raising and advice on how to develop contingency plans.

3. The streamlining of national crisis management to take into account cross-sector crises.

Box 4.1. The different stages of a crisis

Incident phase

An information security incident is usually characterised as a security event that leads to a system or service malfunction. The malfunction may be procedural as well as technical. The impact of an incident on the organisation is generally limited even if the scale is important, as in the case of a computer virus – provided of course that the incident is rapidly contained. The key factors for this are early detection and prompt action. CERT-type structures can provide early warning and assistance to mitigate the effects of some technical information security problems such as viruses, programming weaknesses and errors. They can also act as a conduit for some of the solutions such as virus prevention updates, software "patches" and workarounds. What CERTs cannot do is actually manage the incident in the organisation's operational business environment.

The majority of information security incidents develop into emergencies because of information security management failures such as not responding in a timely manner, or not having procedures and mechanisms in place to react. In some cases, however, inappropriate response can substantially aggravate the problem, as when the application of untested patches causes software failures in customised applications.

Emergency phase

An information security emergency usually develops as a result of an untreated or out-of-control incident that leads to a serious interruption of the organisation's processes. In the worst cases, the response will be to activate business continuity plans. Whereas an incident can be managed locally by IT staff, perhaps with outside assistance, the severity of the impacts of an emergency makes management a matter of organisation-wide decisions. It is therefore important to identify in advance the threshold at which management responsibilities shift.

Similarly, the distinction between emergency and crisis is a matter of the consequences and control. Emergencies are always internal and within the control and responsibility of the enterprise or organisation. The four characteristics that transform it into a crisis are speed, scale, type and impact. Many crises develop because of the failure of untested continuity plans or the absence of continuity plans.

Crisis phase

In a crisis, the organisation itself is at risk. In a company, the disruption of business may threaten the continuity of supply causing loss of business, damage to reputation and possibly exposure to litigation. For a government, many issues are similar. Crisis communication and relations with the media are an inherent part of crisis management. A variety of unexpected knock-on effects with economic, political and social consequences can arise, and the flexibility of government becomes a crucial factor of success. Many disaster situations in recent years have demonstrated the need for responsiveness and leadership at the highest level of the government.

Source: OECD (2004d)

4.1. Incident management

4.1.1. Statement of the issue

Incident detection and vulnerability reduction through software patch management and similar measures are crucial to reducing the significance of an IT incident, stopping it from spreading to other networks, and ultimately preventing its development into an emergency.

Computer Emergency Response Teams (CERTs) typically carry out such tasks, and effectively constitute the first line of defence against general malicious IT activity. The usual tasks of CERTs include the analysis and reduction of IT threats and vulnerabilities, and disseminating warning information. At the national level, CERTs may also have a co-ordination function when it comes to incident response activities. Box 4.2 briefly reviews the experience of some countries in establishing and operating CERTs, and the good practices that are emerging in this area.

Box 4.2: Good practices in establishing and operating CERTs

The first CERT organisation, CERT® Coordination Center (CERT/CC), was established at Carnegie Mellon University in November 1988, after the "Morris Worm" brought down much of the Internet and demonstrated the growing network's susceptibility to attack. Shortly after, the US Defense Advanced Research Projects Agency (DARPA) charged the Software Engineering Institute (SEI) with both establishing a capability to quickly and effectively coordinate communication among experts during security emergencies in order to prevent future incidents, and building awareness of security issues across the Internet community.

Over the past 17 years, CERTs have evolved with the increased use of IT in society. Their main role continues to be the identification and reporting of technical errors and flaws in computer code, but they are no longer restricted to academic environments. Universities conducting IT research still provide some CERTs to support the applications that they develop, but other CERTs have come into being in the development laboratories of major IT suppliers. Furthermore, many large organisations, for example banks, now develop customised versions of information technologies and have also established CERTs within their own organisations. In such organisations, the role of CERTs is not restricted to incident reporting, but also includes giving expert support to the IT operations emergency team dealing with an IT incident. The Forum for Incidence Response and Security Teams (FIRST), which is the leading international organisation of CERT teams across the world, today has over 170 members.

A number of features are starting to emerge as good practices in establishing and operating CERTs, although such a notion can only be relative considering the large variety and uses of CERTs.

First, the CERT should be in close contact and communication with information security specialists who have knowledge of the relevant IT threats, in order to have a notion of the practical consequences of an information system vulnerability. The announcement of a technical vulnerability may create fear, concern and uncertainty among users when in reality there is little or no risk, because there is no practical threat that can exploit the vulnerability. Cryptography is one field particularly affected by this. The ideal CERT should be able to distinguish between what is academically possible and what consequences are likely in practical terms.

Second, the CERT needs to have good knowledge of the business sector where the technology is used and express its advice in terms that business managers and government officials can understand and use to make decisions such as declaring an IT emergency.

Third, the CERT needs to be available outside normal business hours, something that implies adequate financial and technical expert resources.

Fourth, the CERT needs to be part of an international network, so that it does not operate in isolation.

Fifth, the CERT needs to add clear value to the customers it supports, i.e., it needs to have been created with a clear objective in mind, and be allocated adequate resources to attain this. Without this added value, it is unlikely to last over the long term.

Sources: www.uscert.gov , www.cert.org and www.first.org

Small and Medium-sized Enterprises (SMEs) need to be paid particular attention in incident response support. Numerous studies have shown that SMEs are more vulnerable than others in crisis situations. They are normally less well prepared than larger companies, have less expertise and incident management resources, and have less financial resources to cover losses due to interruption of business. As a result, the risk of business failure is higher for SMEs than for larger companies. Availability is generally the most important aspect of information security to an SME dependent on IT systems. Internet-based businesses need access to communicate with their customers, but also their suppliers, banks and service providers. In some cases, confidentiality may also be a concern (for example in the health sector).

A major problem for SMEs is the lack of reliable information and knowledge about how to respond. The cost of getting outside expert support for this activity is usually prohibitive. In emergency or crisis situations where Internet connections might fail, governments often have difficulties reaching out to SMEs. The consequence is that many SMEs with limited resources are forced to stop working until the crisis is over.

Today there are few government-led activities related to incident management and response for SMEs, with most governments focussing their attention on targeted awareness-raising programmes. There are some examples of sector-led activities and some local chambers of commerce and trade associations have encouraged self-help communities of SMEs. These structures contribute to the sharing of knowledge, skills and experience; to organising first line help and support; and possibly to providing more technical second line support, information back-up and equipment sharing. In some communities, one or more members may have the necessary skills and experience to act as an incident focal point providing valuable local knowledge and communications.

Furthermore, there are many instances within an industry where otherwise competing companies will pool their forces in the area of information security. In order to minimise any disruption of operations that might be caused by a virus or worm, multinational companies' CERTs share information security information as quickly as possible.

4.1.2. Policy analysis

In Norway, the lack of a CERT for government services and critical infrastructures has only been addressed gradually. Until recently, Norway had only one CERT member of the Forum for Incidence Response and Security Teams (FIRST), namely the UNINETT CERT, oriented towards academic and research institutions in Norway. The NorCERT project was established within NSM in 2004, became a member of FIRST and linked to the already existing VDI, a 24/7 national warning and information-sharing system for IT threats and incidents. One of the major advantages of NorCERT, related to its anchoring in NSM, is access to sensitive threat information and military expertise. In August 2005, NorCERT was endorsed by the government as the prime national CERT, in charge of co-ordinating incident response activities at the national level.

Although the operation of NorCERT will certainly strengthen incidence response for critical infrastructures in Norway, a number of issues remain. Will NorCERT assure adequate incident management support to all organisations and businesses of "critical" importance to national functionality and security? To what extent will it be able to give high-value specific information about threats and vulnerabilities to a variety of sectors, each with its specific security needs and vulnerabilities? Has the need for sector-specific CERTs with international connections been overlooked?

The current membership model of NorCERT and VDI rests upon an understanding of information security in critical infrastructures that might be too narrow in focus. As stated earlier in this report, there seem to be organisations in Norway with significant importance for society that are not covered by the current scheme, e.g., government social services.

Regarding the specific needs of SMEs, the Norwegian Industrial Safety and Security Organisation (NSO) provides some counsel to private companies, but its resources and expertise in this area seem inadequate, and its service is not available 24/7. The SIS has been confirmed as a focal point for SMEs, but its activities are focussed on awareness-raising and information-sharing, and it does not have response support capacities.

4.1.3. Conclusion and recommendations

Findings

While the impact of a major information security crisis on SMEs and on society as a whole would probably be considerable, there are few incentives for the private sector to create an incident response function.

Opportunities for action

To address this capacity gap it is suggested that the Norwegian government create a CERT specifically aimed at the needs of the private sector, in particular SMEs, in connection with SIS and NSO (see Recommendation 11).

Recommendation 8: Encourage the development of incident response support for SMEs.

4.2. Contingency and preparedness planning

4.2.1. Statement of issue

Crises are often linked to the breakdown in a supply chain, following failure to manage an incident or the combination of a number of incidents. Preparedness and contingency planning are therefore essential measures to prevent a crisis or mitigate its effects. In the public sector and in critical infrastructure components of the private sector, preparedness and contingency planning can be regarded as no more than applying "due diligence" at national level. But in practice, experience shows that contingency plans are not always developed and updated. This may be the result of a lack of awareness, cost and time considerations, or lack of expertise.

Governments therefore must ensure that appropriate contingency plans are in place in the critical segments of the public and private sectors. One policy option for this is to put in place an audit process for critical infrastructures, provide assistance in elaborating plans, and reinforce awareness-raising and consultative efforts to inform users about contingency plans and preparedness planning.

4.2.2. Policy analysis

In Norway, contingency planning to ensure availability and supply is well established in telecommunications and power supply. It is, however, difficult to evaluate if all critical sectors have the same level of preparedness. There are strong indications that Norwegian policy in the area of preparedness and contingency planning for IT crises is incomplete. As mentioned in chapter 3, responsibilities with regard to audits are piecemeal. In particular, there is no public institution with a mandate to audit IT contingency planning in private critical infrastructures that handle non-classified information. Information security preparedness and contingency planning also seem less mature in government services which are less concerned by the Act Relating to Protective Security Services.

A number of users in the Norwegian public sector acknowledge their need for help and assistance from other expert agencies regarding IT threats (NSM, for instance), in order to develop credible threat scenarios and improve their organisation's preparedness level.

4.2.3. Conclusion and recommendations

Findings

There is a gap in responsibility regarding consultancy and audit of contingency planning for private critical infrastructures and public services that do not manage classified information.

Two major candidates for giving advice on information security preparedness, contingency planning and threat scenarios, namely NSM and DSB, are also in charge of audits.

Opportunities for action

- The government could develop a consultancy capability for users in the public and private sectors in order to encourage the creation of contingency plans.

- A government auditing function could be extended to include critical infrastructures, irrespective of whether they are publicly or privately owned or operated, and whether they manage classified or non-classified information. Private audits could also be used.

- In parallel, the government could also consider the principle of separation of the audit and consultancy functions, which has become commonplace and often mandatory in the private sector.

Recommendation 9: Strengthen government consultancy and auditing services in order to promote preparedness and contingency planning.

4.3. Emergency and crisis management

4.3.1. Statement of issue

Governments usually have well established procedures for declaring emergencies and managing them. The four characteristics that can make an information security emergency a crisis are speed, scale, type and impact. The speed at which an Internet virus or worm can infect computer systems is almost real time. The scale can be global. It is the impact that will determine when and whether an information security emergency transforms into a crisis, thus requiring government intervention. In short, an IT emergency might be considered a crisis when:

1. It spreads very quickly.

2. It is on a national or international scale.

3. It potentially disrupts or undermines essential government or societal services.

4. The severity of the impact creates a significant threat to society at large for reasons of safety or security.

4.3.2. Policy analysis

Crisis management in Norway is subject to the rule of sector responsibility, and the lines of responsibility and command remain the same in an emergency as in day-to-day operations. This is justified by the assumption that crises are best managed by those who know the systems and functions intimately. However, a major emergency is very likely to affect many different sectors at the same time. It is an increasingly common feature of "modern" disasters that they have numerous and unexpected knock-on effects. The experience of IT crises in other countries, e.g., related to power blackouts and terrorist actions, demonstrates that there are many unpredictable effects of a crisis across both the public and private sectors, because the direct and indirect dependencies on IT are not always known. In such cases, experience shows that there needs to be a single focal point for all stages of crisis management. This is the only effective way to set priorities across ministerial departments, to manage the crisis situation in partnership with the affected organisations, and to communicate with the public and the media.

The existence of effective cross-ministerial IT incident, emergency or crisis management in Norway is open to discussion. Informal modes of communication are mentioned as an effective tool for co-ordination, but there is a lack of an authoritative body in charge of actual co-ordination. The Cabinet Emergency Council created in 2005 could fill this gap, provided that its scope extends to information security crises, and it is vested with the actual authority and control of decision channels to overcome sector divergences in emergency situations.

4.3.3. Conclusion and recommendations

Findings

A centre for national crisis management can play a vital role in monitoring an IT crisis as it develops and in mitigating the effects if it develops beyond the stages of incident or emergency.

Opportunities for action

To be most effective the “core” members of a centre for national crisis management should have the collective authority to direct and manage resources once a crisis has been declared. This authority and the declaration of such a crisis may need to be supported by parliament and relevant crisis management legislation. This centre could be a component of the newly created Cabinet Emergency Council (see also Recommendation 5).

Recommendation 10: Create a national IT crisis management capability.

Chapter 5. Strengthening the Foundations of Security

In its investigation of national initiatives to implement the OECD Guidelines for the Security of Information Systems and Networks, the OECD Secretariat identified awareness-raising, information-sharing (in CERT-type structures) and education as three fields where OECD member countries have focussed their efforts in order to promote a culture of security. In addition to these, "there is a consensus among responding countries to recognise the importance of research and development activities for fostering the security of information systems and networks." Nevertheless, publicly funded or supported programmes of R&D are still very limited in OECD countries (OECD, 2005a).

5.1. Awareness-raising

5.1.1. Statement of the issue

There are two aspects to raising awareness. One is raising the sensitivity of citizens and corporations regarding the risks of inadequate information security. The other is giving advice on best practices for reducing the risks to an individual or corporation to acceptable levels. These policies should be considered complementary and using one policy without the other should even be considered detrimental, as shown by the findings of e-Aware, a research project on awareness-raising among 10 European countries (OECD, 2004c).

First, awareness-raising without information on response options can cause alarm among users. This situation characterised the early days of electronic commerce on the Internet, when credit card users were discouraged by their banks on the grounds of the information security risks. The impact was to slow the growth of the Internet-based economy. It was only after a lot of effort to educate users on the actual consumer liabilities and the adequacy of security on secure websites that the IT risks were put into perspective and users had confidence to conduct business over the Internet. Only then did the Internet economy really start to grow.

Second, giving advice on response measures without raising awareness can lead to complacency about the actual risk landscape. The credibility of the source of the advice is also undermined for "crying wolf".

Individuals, in their day-to-day use of IT, also need a basic understanding of threats and vulnerabilities in order to make an informed assessment of their individual risk. Heightening sensitivity about the threat without relating it to a vulnerability, or vice versa, can also be negative. Citizens and corporations need to have a clear picture of both the threat and the vulnerability that can be exploited in order to ascertain the level of risk they must contend with. Detailed knowledge and experience is scarce in an average user population, which will normally have to depend on experts for advice. Governments can provide impartial advice at low cost, and government promotion of awareness and advice for responding (including compliance with relevant legislation) is essential to the protection of information systems in society as a whole. In this way, individuals and SMEs have sufficient information to make decisions about the general information security measures that need to be put in place. For example, most small business or individual computers now have an information security software package installed to protect against unwanted intrusion and computer viruses.

Most OECD countries have launched awareness-raising campaigns in recent years. Initiatives of interest were reviewed recently by the OECD Secretariat within the framework of the Working Party on Information Security and Privacy (OECD, 2005a). Typical actions include conferences, publications, and special web sites and portals, etc. Communication has targeted the general public, or in some cases, more restricted audiences such as businesses, SMEs, new users, and young people. In Germany, for example, 1 million CD-ROMs have been distributed, and, in partnership with a major computer manufacturing company, background information has been preinstalled on new computers.

5.1.2. Policy analysis

For individuals, businesses, and other organisations, security needs to become an integral part of the normal way of using IT and doing e-business. A process of learning and self-improvement, based on sharing of experiences, has to be encouraged; and a shift in thinking by policy-makers is probably also needed. These steps are all part of creating an information security culture.

Past efforts to raise awareness and promote a culture of security have had mixed results, with the notable exception of the NettVett information website, launched by the Norwegian government in April 2005. The NettVett website is managed by the Post and Telecommunications Authority, and a series of stakeholders have provided input, including the Ministry of Modernisation, Data Inspectorate and SIS on the public side, as well as business actors and special interest groups such as the NSR (Norwegian Industrial Security Organisation). Consumer organisations have also contributed. The website gives information about different information security topics and adapts it according to user group (individuals with little/normal IT knowledge, business managers, parents, etc.).

Some end users and system operators demonstrate a low level of knowledge of good security practices, available solutions, business continuity, etc. This includes government departments in charge of important information systems, which rely on their own individual initiatives to maintain a satisfactory level of security (in accordance with the principle of sector responsibility).

In addition, the authorities need to investigate the dependence of Norwegian SMEs on IT, and contribute to and support the collection of incident reports and useful statistics in order to establish the extent of damage caused by malware in the private sector. In this regard, the survey on computer crime is an important initiative (Røstad and Eilertsen, 2004). The survey is a result of co-operation among the SIS, NSR and the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM). The survey started in the early 1990s and is now carried out every second year. It provides a valuable contribution to the current picture of active threats in the Norwegian IT environment.

5.1.3. Conclusion and recommendations

Findings

Awareness-raising is effective only if accompanied by incident support and the promotion of solutions. In this respect the launch of NettVett and the decision to make SIS a permanent organisation primarily oriented towards SMEs are positive steps.

Opportunities for action

- In order to sustain recent progress in outreach to small businesses and the general population, the authorities could put the funding of SIS and NettVett on a sound, long-term footing.

- Partnerships could be developed through SIS in order to support outreach to business and civil society.

- The creation of a CERT-type structure dedicated to SMEs could help to promote solutions at the same time as increasing awareness about risks (see Recommendation 8).

Recommendation 11: Improve and rationalise awareness-raising efforts directed towards SMEs and the general public.

5.2. Information-sharing

5.2.1. Statement of the issue

The pace of development and change in IT sets it apart from any previous technical revolution. An Internet "year" or "technical generation" in development terms is generally considered to be 100 days. In addition, IT development engineering is driven more by practice than theory. Commercial pressures of survival often mean that the next generation of technology is on the market before it has been thoroughly tested and all security weaknesses ironed out. This environment makes acquiring the necessary knowledge and skills in information security in a classical manner impossible. Even experienced information security experts have to run to keep up with the changes.

In this environment, the critical success factor in information security is rapidly sharing information and experience. Large organisations, including governments, can afford to have dedicated information security experts to monitor and share information on changes in IT in order to provide early warning of the threats and vulnerabilities affecting the next generation. Private citizens and SMEs do not have this luxury. Instead, they face a barrage of stories on information security from the media. The pace of change means that experts debate the significance of a risk without reaching a conclusion because the discussion is overtaken by a new development. This leaves the citizen and SME confused, and is made worse by the partiality of some discussions, which can have more to do with promoting commercial or personal interests than with the practical use of IT. Governments can play a number of valuable roles in encouraging and facilitating the sharing of knowledge and experience. First of all, they can set an example by sharing their own information with the private sector. Government information security experts can also use their impartial position to provide useful guidance to citizens and SMEs. This guidance will help to put order and balance into the mass of information on IT security.

5.2.2. Policy analysis

Many governments have created information and experience sharing groups. These tend to be either business sector or technology centred. The most effective groups are made up of government regulators, business users and technology suppliers meeting with equal status. 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 Centres (ISAC), industry-specific networks for disseminating up-to-date information, sharing experiences, and promoting industry-government co-operation based on trust in the field of information security (ISAC Council, 2004b). ISACs are a common form of industry organisation in the United States, in particular for critical infrastructure sectors. In April 2004, 15 critical infrastructure ISACs were identified in the country, including in financial services (the first of all the ISACs, established in 1999), telecommunications and electric power generation. Most of them address cyber-threats and are supported by government funds (United States General Accounting Office, 2004b, pp. 18-22).

In the United Kingdom, two alternative forms of information-sharing structure are supported by the government (specifically by the National Infrastructure Security Co-ordination Centre) (Comprehensive Risk Analysis and Management Network, 2004, p. 193). 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). Warning, Advice and Reporting Points are small, interlinked, community-based information-sharing cells, conceived as a cost-effective alternative to ISACs.

The success or otherwise of these groups can be measured by how well they manage a number of sensitive issues. Government security agencies are reluctant to share threat information on the grounds of national security and protecting their sources. Businesses are reluctant to share information on business impact that might be regarded as harmful to their business by exposing management weaknesses or deficiencies, possibly resulting in adverse publicity, litigation or financial losses. Technology suppliers are reluctant to disclose any information on vulnerabilities that might harm their sales or expose them to litigation or reduce sales. An evaluation of ISACs in the United States by the US General Accounting Office revealed two main problems: ISACs had variable degrees of outreach and membership (the electricity ISAC had almost 100 percent membership, while the members in the Financial Services ISAC represented only 0.2 percent of all entities in the sector); and trust was still relatively low. The main obstacles to information-sharing were concerns over possible government release of information and the limited quality of government information (US General Accounting Office, 2004b). In response to this, the US government has decided to restrict public access to sensitive information provided by critical infrastructure operators.

In Norway, as described earlier, roles and responsibilities are to a large extent allocated vertically across the various government sectors, with only loose co-ordination forums operating across sectors on matters related to national security, which is generally restricted to protecting confidentiality. Such a general architecture can inhibit the exchange of information and best practices among users. Degrees of maturity differ widely from one government organisation to another, e.g. in the use of standards.

The main information-sharing structures are NSM's Warning for Digital Infrastructures (VDI) and the SIS Reference Groups. The latter are an ambitious and bold initiative for encouraging information-sharing within industries, but their development seems hampered by inadequate support at the policy-making level. There seems to be a lack of co-ordination between the individual Reference Groups and VDI, and hence a lack of clarity regarding the respective functions of the two entities.

5.2.3. Conclusion and recommendations

Findings

There is a fair amount of knowledge and experience of information security in individual ministries and agencies, but opportunities to share this knowledge are restricted in some cases by the existence of sector-specific ministerial "silos". Improvements could be made in stimulating the exchange of information and best practices among users on how to secure their networks and information systems, according to their individual level of maturity regarding information security.

Opportunities for action

- A low-cost option for providing support platforms for SMEs would be to sponsor, encourage and promote small, local self-help groups, supported with external advice from experts in government and universities.

- The roles of open and closed forums could be more clearly differentiated according to the level and sensitivity of the information exchanged.

- SIS and NorCERT could be used as more active and wide-ranging platforms for information-sharing for all types of end users, with specific tools for different target groups: individuals, SMEs, public administrations, etc. (see also Recommendation 11).

Recommendation 12: Stimulate the exchange of information and best practices among users.

5.3. Education and R&D

5.3.1. Statement of the issue

As stated earlier, education and training appear to be one of the pillars of governments' efforts to promote a culture of security. Initiatives in this area include the free distribution of educational material, the use of Internet forums, measures oriented towards school teachers, etc. National curricula are being adapted in order to improve knowledge of information security in the population and to educate future information security managers.

In comparison, OECD countries have paid relatively little attention to supporting R&D in information security. Research is often undertaken as part of broader research programmes, and its focus is computational and technological, with less consideration for other aspects of relevance for policy-making, including the environment in which the security tools might be used. Existing research programmes are usually conducted within national academia, with few examples of co-operation with government, industry or international partners.

Inadequate interaction between research in information security and end users of that research is clearly non-optimal. Close liaison between researchers and industry can help provide early warnings and solve technical security problems. Research could also identify best practice and communicate it quickly to government and society. Research could also help to identify national critical infrastructure needs and give advice to policy-makers on how to respond. Research programmes could directly contribute to the realisation of the national information security strategy by identifying and proposing solutions to actual and potential threats and vulnerabilities.

In turn, governments and industry could provide increased support for security-enhancing education and R&D, notably by prioritising information security in their own research agendas, or through public-private partnerships.

One example is the US National Strategy to Secure Cyber-Space, which comprises the elaboration of a federal government information security research agenda covering issues such as intrusion detection, Internet infrastructure security, application security, denial of service, and high-assurance systems (United States, President, 2003). In addition, the plan charges the Department of Homeland Security with reviewing, and if necessary developing, mechanisms of co-ordination for research and development among academia, industry and government.

In Germany, the Federal Office for Information Security (BSI) runs several projects in partnership with industry on topics including penetration testing, early warning, biometrics, and cryptography.

5.3.2. Policy analysis

Norway has recognised the need to create a literate and skilled population in the field of IT. This includes plans to create a teaching package for information security to be used along with teaching IT at every level of education in the country. In the future, these plans will lead to information security being taught as a separate discipline. In the long term, this should contribute to raising the awareness of citizens and equipping them with the basic knowledge and skills to manage information security. Specialist courses at university, including masters degrees in information security, will provide the necessary experts and specialists. Experience from the introduction of IT shows that the benefits of these measures will become embedded in society in the next generation of the workforce.

Concerning research, there seems to be a missing link between policy-makers in charge of implementing the National Strategy and R&D programmes. In the IKT SoS project, research proposals have been put forward mainly by the research community with little direction given by policy-makers or users. Such a “bottom-up” approach to defining the content of research programmes has obvious advantages, but it could also have two major shortcomings. First, as mentioned, it could limit the usefulness of research for end users – indeed, most projects funded by IKT SoS focus on fundamental rather than applied research. Second, it could create a bias towards areas that are already well covered by the national research community at the expense of new areas of interest. One exception is the BAS5 project, which was initially based on a well-identified need, but has since suffered from a profusion of stakeholders with differing priorities.

As a result, too little attention is devoted to encouraging innovative applications that would directly target the goals established by the National Strategy. Given the scarcity of resources (the IKT SoS research budget for information security represents 0.3 percent of the annual budget of the Norwegian Research Council), it is crucial that research programmes on information security are very carefully targeted to accommodate national strategic needs. Thus, the key expression in the future orientations of research could be "enabling the Strategy".

Information-sharing with the relevant government departments and agencies could be a mandatory condition of any research sponsorship agreement in this area.

When research programmes are oriented towards a specific issue or solution, their monitoring would be facilitated if the programmes had to include an exploitation plan from the outset, so that their expected benefits and beneficiaries were clearly identified. The BAS5 project seems to suffer from the lack of such requirements for specific deliverables, which would explain the gradual changes in its content, objectives, and resources.

5.3.3. Conclusion and recommendations

Findings

The connection between research and the Norwegian information security strategy is tenuous, and the ultimate beneficiaries of research seem to have limited possibilities to influence the content of research programmes.

Where research programmes are oriented towards a specific issue or solution, their monitoring could be better facilitated if the programmes included an exploitation plan from the outset. The expected benefits and beneficiaries would then be more clearly identified. The BAS5 project seems to suffer from the lack of such requirements, which possibly explains the gradual shift in its content, objectives, and resources.

Opportunities for action

- Information-sharing with the relevant government departments and agencies could be a mandatory condition of any research sponsorship agreement in this area. Such connections were not found in either of the research initiatives considered.

- A national strategy on information security research would help to identify gaps, prioritise resources, guide research programmes and identify areas where co-operation with foreign counterparts might add most value.

- Potential users and beneficiaries of research could be given a greater role in the definition and guidance of research programmes. The KIS is one possible forum for this type of activity provided that the private sector is more specifically involved. The KIS could also be given the opportunity to commission, fund and evaluate research, in order to make more use of the demand side to guide research programmes.

Recommendation 13: Define a national strategy on information security research, and enhance the role of the demand side in guiding research projects.

Bibliography

British Standards Institution (BSI) (2002), *BS7799 Part 2: Information security management systems – specification with guidance for use,* BSI, London.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2004), *Analysis of Critical Infrastructures – The ACIS methodology*, briefing document, BSI, Bonn.

Central Information Systems Security Division (SGDN/DCSSI). (2004), *Expression of Needs and Identification of Security Objectives – ENISO*, Secrétariat Général de la Défense Nationale, Paris. www.ssi.gouv.fr/en/confidence/ebiospresentation.html, accessed 15 March 2006.

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

Comprehensive Risk Analysis and Management Network (2004), *International CIIP Handbook 2004,* Center for Security Studies, Swiss Federal Institute of Technology, Zurich.

Computer Security Institute (CSI)/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 DC 1 April 2004, cited in General Accounting Office (GAO) report 04-706: *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO, Washington DC.

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

European Commission (2001), *Network and Information Security: Proposal for a European Policy Approach,* EU Commission Communication, COM(2001)298, Brussels.

European Commission (2004), *Critical infrastructure protection and the fight against terrorism,* EU Commission Communication, COM(2004)702, Brussels.

European Commission (2005), *Draft Commission decision on the application of Article 86(2) of the Treaty to State aid in the form of public service compensation granted to certain undertakings entrusted with the operation of services of general economic interest*, available at http://europa.eu.int/comm/competition/state_aid/others/action_plan/sgei_art86_en.pdf, accessed 17 November 2005.

Fischer, Dennis (2003), "New Dangers Exposed in the Wake of Slammer", *E-Week*, 3 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", *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.

Grall, Matthieu (2005), "Managing Risks with the EBIOS Method", *ENISA Quarterly*, 12/2005, available at http://www.enisa.eu.int/doc/pdf/publications/enisa_quaterly_12_05.pdf.

Gulichsen, Steinar et al. (2004), *Strategier for informasjonssikkerhet – en komparativ studie av strategiarbeidet I Norge, USA, Australia og EU*, Norwegian Defence Research Establishment, Kjeller.

Harris, Robert 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.

Hoo, Kevin J. Soo (2000), "How Much is Enough? A Risk Management Approach to Computer Security", Consortium for Research on Information Security Policy (CRISP) Working Paper, Stanford University, Stanford.

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

International Organization for Standardization (ISO) (2002), *GUIDE 73: Risk management —Vocabulary — Guidelines for use in standards*, ISO, Geneva.

ISAC (Information Sharing and Analysis Centers Council) (2004a), “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 (2004b), *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.

Mi2g (2004), “Economic Damage from Bagle, MyDoom & NetSky crosses $100bn: Financial Motive behind the Malware Variants Likely”, News alert, 8 March 2004, available at www.mi2g.co.uk, accessed 11 August 2004.

National Research Council (1991), *Computers at Risk: Safe Computing In the Information Age*, National Academy Press, Washington DC.

National Research Council (2002), *Cybersecurity Today and Tomorrow: Pay now or Pay Later*, National Academies Press, Washington D.C.

National Research Council (2003), *Information Infrastructure Protection and the Law: An Overview of Key Issues*, National Academies Press, Washington DC.

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

Netherlands Ministry of the Interior and Kingdom Relations (2003), *Critical Infrastructure in the Netherlands*, Ministry of the Interior and Kingdom Relations, The Hague.

Norwegian Financial Supervisory Authority (2004), *Risk and Vulnerability Analysis 2004 - the Finance Institutions' Use of ICT,* Kredittilsynet, Oslo.

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

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

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

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

Norwegian Ministry of Modernisation (2005*), eNorge 2009, Implementation Plan*, Ministry of Modernisation, Oslo.

Norwegian Ministry of Trade and Industry (2000), *Samfunnets sårbarhet som følge av avhengighet til IT*, Ministry of Trade and Industry, Oslo.

Norwegian Ministry of Trade and Industry (2002), *eNorge 2005*, *Implementation Plan*, Ministry of Trade and Industry, Oslo.

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

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

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

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris.

OECD (2003a), *A Methodological Framework for Evaluating Risk Management Policies*, background document, first meeting of the Steering Group of the OECD Futures Project on Risk Management Policies, 3 November 2003.

OECD (2003b), *OECD Reviews of Regulatory Reform: Norway, Preparing for the Future Now,* OECD, Paris.

OECD (2003c), *Emerging Risks in the 21st Century: An Agenda for Action,* OECD, Paris.

OECD (2004a), *Risk Management Policies in Norway Concerning Information and Communication Security,* OECD Studies in Risk Management, OECD, Paris.

OECD (2004b), *Summary of Responses to the Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, DSTI/ICCP/REG(2003)8/ FINAL, OECD, Paris

OECD (2004c), OECD Global Forum on Information Systems and Networks Security: Towards a Global Culture of Security. Proceedings. 13-14 October 2003, Oslo, DSTI/ICCP/REG/2004/1. OECD, Paris.

OECD (2004d), *Large-scale Disasters: Lessons learned,* OECD, Paris.

OECD (2005a), *Draft report on the promotion of a culture of security for information systems and networks in OECD countries,* DSTI/ICCP/REG(2005)1/REV2, classified document, OECD, Paris.

OECD (2005b), *OECD e-Government Studies, Norway,* OECD, Paris.

Poulsen, Kevin (2003), "Slammer Worm Crashed Ohio Nuke Plant Network", *Security Focus,* 19 August 2003, available at http://www.securityfocus.com/news/6767, accessed 11 August 2004.

Quebec Ministry of Public Security, (1999), *Commission scientifique et technique chargée d'analyser les événements relatifs à la tempête de verglas survenue du 5 au 9 janvier 1998* (Commission into the 1998 ice storm in Quebec).

Røstad, L. and Ø. Eilertsen (2004), *Mørketallsundersøkelsen 2003 – om datakriminalitet og IT-sikkerhet*, Næringslivets sikkerhetsråd, NorSIS, Gjøvik.

United States General Accounting Office (2002), *Critical Infrastructure Protection: Federal Efforts to Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO Report GAO-02-474, July 2002, Washington D.C.

United States General Accounting Office (2004a), *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO report GAO-04-354, Washington D.C.

United States General Accounting Office (2004b), *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*, GAO report GAO-04-699T, Washington D.C.

United States General Accounting Office (2004c), *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO report GAO-04-706, Washington D.C.

United States General Accounting Office (2005), *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity,* GAO Report GAO-05-827T, GAO, Washington D.C.

United States Office of Management and Budget (2005), *Federal Information Security Management Act (FISMA), 2004 Report to Congress,* available at http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf, accessed 18 November 2005.

United States, President (2003a), *The National Strategy to Secure Cyberspace*, The White House, Washington D.C.

United States President (2003b), *The US government's National Strategy for Physical Protection of Critical Infrastructure and Key Assets*, Washington D.C.

Annex 1: Terminology and Definitions

Asset: Anything that has value to the organisation (ISO/IEC TR 13335).

Availability: The property of being accessible and usable upon demand by an authorised entity (ISO 7498-2: 1998).

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

Baseline controls: A minimum set of safeguards established for a system or organisation (ISO/IEC TR 13335).

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities, or processes (ISO 7498-2: 1988).

Critical Infrastructures: Infrastructures (physical and applications) without which society cannot function adequately, such as water supply, food supply, transport, public health, telecommunications, etc.

***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 modem, 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 forms (.com, .net, etc.) as well as the country code top-level domains.

Due diligence: A general duty to take every precaution reasonable in the specific circumstances (health and safety, national security, etc.); a defence if charged with a breach of legal duty.

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.

Integrity: The property of safeguarding the accuracy and completeness of assets (ISO/IEC TR 13335).

***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 (see entries below).

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 threat.

Risk assessment: The process of gathering information regarding risk before taking any decision relative to its handling.

***Risk**:* The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation (ISO/IEC TR 13335).

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 assessment: Collection of information on the extent of damage that might be caused to a population or system by a certain hazard.

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 website 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.

Annex 2: Acronyms and Organisations Cited

BAS *(Beskyttelse av samfunnet)*: Protection of society

CERT: Computer Emergency Response Team

CERT/CC: CERT Coordination Center (Carnegie Mellon University, United States)

CIP: Critical infrastructure protection

CIIP : Critical information infrastructure protection

DSB *(Direktoratet for samfunnsberedskap)*: Directorate for Civil Protection and Emergency Planning

Datatilsynet: Data Inspectorate

ENISA: European Network and Information Security Agency

FFI (*Forsvarets forskningsinstitutt*): Norwegian Defence Research Establishment

FISMA: US Federal Information Security Management Act

GAO: General Accounting Office (United States)

ICT: Information and Communications Technologies

ISAC: Information Sharing and Analysis Centre

KIS *(Koordinasjonsutvalg for informasjonssikkerhet*): Coordination Group for Information Security

MoD (*Forsvarsdepartementet*): Ministry of Defence

MoJ (*Justis- og politdepartementet*): Ministry of Justice and the Police

MoM (*Moderniseringsdepartementet*): Ministry of Modernisation

MTC (*Samferdelsesdepartementet*): Ministry of Transport and Communications

MTI (*Nærings- og handelsdepartementet*): Ministry of Trade and Industry

NISCC: National Infrastructure Security Co-ordination Centre (United Kingdom)

NIST: United States National Institute of Standards and Technology

NPT (*Post- og teletilsynet*): Norwegian Post and Telecommunications Authority

NSM (*Nasjonal sikkerhetsmyndighet*): National Security Authority

NSO (*Næringslivets sikkerhetsorganisasjon*): Norwegian Industrial Safety and Security Organisation

NSR (*Næringslivets sikkerhetsråd):* Norwegian Industrial Security Organisation

OMB: Office of Management and Budget (United States)

Norsk Forskningsråd: The Research Council of Norway

SCADA: Supervisory Control and Acquisition

SIS (*Senter for informasjonssikring*): Centre for Information Security

SME: Small and medium-sized enterprise

US-CERT: United States national CERT

VDI (*Varslingssystem for digital infrastruktur)*: Warning system for digital infrastructure

WARP: Warning, Advice and Reporting Points

Annex 3: Methodology

The review process

In April 2004, in the framework of the OECD Futures Project on Risk Management Policies, the Norwegian Ministry of Justice and the Police asked the OECD Secretariat to elaborate "an assessment of information and communication technology security measures with an aim to developing optimal broad-spectrum vulnerability reduction."

This mandate followed a two-day workshop organised in March 2004 by Norway's Directorate for Civil Protection and Emergency Planning to which, in addition to the OECD Secretariat, a large number of actors involved in the management of information security were convened. These included in particular the Ministry of Trade and Industry, then in charge of overseeing the implementation of 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 IT security, and confirmed that there was strong interest in a first assessment of these measures.

In February 2005, the OECD Secretariat delivered a study on information security to the Norwegian authorities (OECD, 2004a). It comprised an overview of recent international and national developments of interest, a mapping of institutions involved in the management of information security in Norway,[9] as well as a series of self-assessment questionnaires.[10] The study prepared the ground for an in-depth review of information security management in Norway, using as a starting point the assessment of policy by Norwegian actors themselves.

In April 2005, the Directorate for Civil Protection and Emergency Planning (DSB) organised a second workshop in Oslo, where participants from a broad range of ministries and regulatory agencies had a fruitful discussion with the OECD Secretariat over the review process and the questionnaires. The questionnaires were then sent to all relevant entities, both inside and outside the government, and replies were collected. In June

[9] See Annex 4 to this report.

[10] See Annex 5 to this report.

2005, the review team carried out a one-week mission in Oslo, during which it held twenty interviews with representatives of the Norwegian government, corporations and non-governmental organisations.[11]

The team submitted an interim report of its findings and recommendations to the Norwegian authorities in September 2005, and requested their comments. In December 2005, the team delivered the first draft of this final report.

Overview of the methodology followed to evaluate risk management policies

Risk management is a complex process involving many different phases, from the evaluation of threats and the creation of protection strategies, to understanding liability issues and investigations after a disaster. Failure to complete the entire risk management process can lead to important linkages among these activities being overlooked, thereby undermining the overall effectiveness of a policy. This is the case, for instance, when the assessment of risk is not closely associated with the identification of affordable means of avoidance, or when risk prevention measures are designed with little attention to the actual incentives provided by insurance policies.

In order to address the need for a holistic approach, the OECD Project on Risk Management Policies has developed a methodology (OECD, 2003) which considers risk management as a multi-layered system, where each layer performs a particular function with regard to risk, and provides inputs to some of the other layers:

- Risk or vulnerability assessment.
- Policy decision-making, based on risk assessment and acceptability, and on available options for treating or transferring risk.
- Framework conditions, i.e., laws, norms, and all regulations and public actions that create obligations and incentives with regard to risk.
- Protection, i.e., devices, constructions and procedures to protect exposed populations and systems: dams, shields, shelters, displacement of threatened persons, quarantines, etc.
- Information, i.e., awareness-raising, information-sharing.

[11] See Annex 6 to this report.

- Alert and rescue, to mitigate the immediate impact of hazard.
- Recovery enhancement, to mitigate the longer-term impact of hazard.
- Experience feedback and organisational change.

When elaborating the self-assessment questionnaires, all relevant actors, institutions and rules are considered in each layer. The layer's performance is evaluated against a set of criteria falling under three major headings: coherence of organisation, effectiveness in achieving objectives, and openness to external sources of information. To evaluate the performance of the overall system, the linkages between layers are also investigated through questions such as the management of past crises; the quality of experience-feedback and the capacity to trigger organisational change; the ability to detect changes and to adapt to new conditions; the management of uncertainties and the consistency of precautionary measures; and the existence and pertinence of a risk management strategy.

This approach was applied to the Review of Risk Management Policies in Norway Concerning Information Security, and followed to a large extent in the structure of this report. However, a number of adaptations have been made in order to tailor the review to the specific case of information security in Norway, or simply to improve the readability of the report:

1. Policy decision-making, the framework conditions, and experience feedback and organisational change have been considered jointly as the components of the Norwegian Strategy for Information Security. These layers are addressed in Chapter 1 of the report.
2. Risk assessment is the topic of Chapter 2.
3. The protection layer is dealt with in Chapter 3.
4. Alert and rescue and recovery management have been grouped in Chapter 4.
5. The analysis of research and education policies has been presented together with awareness-raising and information-sharing (information layer) as the "foundations of a culture of security" in Chapter 5.

Correspondence with other methodologies in the field of information security

The broad-based concept of risk management system used in the Project is consistent with the definition proposed by the International Standards Organisation (ISO, 2002): "The set of elements of an organisation's management system concerned with managing risk", where "managing risk" is defined as all "co-ordinated activities to direct and control an organisation with regard to risk."

The layers considered in the risk management system are consistent with most methodological approaches based on the "risk management cycle". An example of these in the area of information security is the "Plan-Do-Check-Act" cycle prescribed by the standard ISO 27001 or BS7799-part 2 for "setting up and managing an effective Information Security Management System (ISMS)", (BSI, 2002):

- The Plan phase consists in establishing the ISMS, i.e., establishing "security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the organisation's overall policy and objectives." In terms of the Project's methodology, these are the risk assessment and policy decision-making layers.

- The Do phase is to implement and operate the ISMS, namely to "implement and operate the security policy, controls, processes and procedures." The Project's emphasis on public policy leads to separating this broad set of actions into several layers: framework conditions, protection, information, alert and rescue, and recovery enhancement.

- The Check phase is to "assess, and when applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review". This corresponds to the feedback layer.

- The Act phase consists in "taking corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS", which is considered by the Project's methodology as organisational change.

Annex 4: Norwegian Institutions and Laws in the Area of Information Security

The following annex briefly describes the sharing of responsibilities in the management of information security in Norway, and the legal and regulatory framework. The description follows the Project's methodology for analysing risk management systems (see Annex 3).

Responsibilities for the management of information security

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 • DSB • NSM • Sector departments (e.g., Post & Telecom Authority)
	Development and promotion of risk assessment tools	• Ministry of Modernisation • 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)

Functional layers	**Actions**	**Authorities**
Framework conditions	Development and use of standards and certification	• Norwegian Accreditation, NSM (SERTIT) • Ministry of Modernisation (private sector and public sector procurement) • Ministry of Defence
	Promotion of security-enhancing technologies	• Ministry of Trade and Industry • 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) • Data Inspectorate (protection of personal data) • Regulatory authorities (each in their area of competence) • Trade organisations, P&T Authority and Ministry of Modernisation (benchmarks for IT vendors and service providers)
Protection	Security of government services	• Ministry of Modernisation (government security guidelines) • Data Inspectorate (secure processing of personal data)
	Security of critical infrastructures	• Ministry of Transport & Communications (robustness of the Internet infrastructure) • Directorate of Social Services and Health (security policy for the health sector) • 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) • DSB • NSM
	Education	• Ministry of Education and Research
Information	Awareness-raising	• Ministry of Modernisation and Ministry of Transport & Communications (information activities) • SIS (dissemination of information, reporting issues) • Norwegian Industrial Safety and Security Organisation and trade organisations (corporate information security guidelines) • Ministry of Modernisation (international co-operation, OECD, ENISA) • Ministry of Transport & Communications (ENISA) • Data Inspectorate (processing of personal data)
	Information- sharing	• NSM / NorCERT • SIS
	Warning	• VDI, SIS, UNINETT CERT, TERT, other CERTs
Rescue	Incident response assistance	• UNINETT CERT • TERT (telecommunications)
Recovery enhancement	Contingency and business continuity plans	• DSB • NSM
Feedback and organisational change	Feedback and learning mechanisms	• SIS (sources of incidents) • ØKOKRIM (investigations) • KIS (organisational change)

The legal and regulatory framework

Principal laws and regulations	Enforcement authorities
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 / NPT
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 5: Self-assessment Questionnaires

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 government 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, sector 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 sector (e.g. Post & Telecom Authority) and cross-sector (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

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 co-operation with structures such as ISACs.

c. What is the degree of centralisation of Information security policy in public administrations at present (e.g. totally centralised, common guidelines with sector 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 co-ordination of Information 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 Information security standards?

g. Please describe government's current and planned actions to encourage the use of standards and certification in the area of information 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, Sector 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 Information 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 government 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 government 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 government 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 government 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 sector (e.g. Ministry of Transport and Communications, Directorate of Social Services and Health) and cross-sector (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-government actors integrated in critical information infrastructure protection activities, and is this co-operation co-ordinated and known to all other government actors in the field?

i. Is there a dialogue between stakeholders (private and public) and government 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 co-ordination 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 co-operation and is this co-operation co-ordinated, 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 programmes been established (e.g. Masters)?

E. Information and early warning

E.1. Awareness-raising

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 co-ordinated 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 Information 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 6: List of Interviewees

Centre for Information Security (SIS)

Ove Olsen, Director

Directorate for Civil Protection and Emergency Planning (DSB)

Arthur Gjengstø, Director
Stein Henriksen, Senior Advisor
Kjetil Sørli, Advisor

Directorate of Health and Social Services

Tor Ottersen, Senior Advisor

Ministry of Defence

Nils Jørgen Bogen, Senior Engineer
Severin Vikanes, Assistant Director General

Ministry of Modernisation

Katarina de Brisis, Senior Advisor
Cort Archer Dreyer, Advisor
Eivind Jahren, Head of Department

Ministry of Transport and Communication

Heidi Karlsen, Advisor
Jørn Ringlund, Head of Section

National Defence Research Establishment (FFI)

Janne Hagen, Principal Scientist
Kjell Olav Nystuen, Principal Scientist

National Insurance Administration

Herbjørn Andresen, Senior Advisor

National Security Authority (NSM)

Kjell Bergan, Head of Section (SERTIT)
Anders Bjønnes, Senior Advisor
Sofie Nystrøm, Manager (NorCERT)
Eiliv Ofigsbø, Head of Section
Jan Tobiassen, Senior Engineer

Norwegian Industrial Safety and Security Organisation (NSO)

Steinar Beck Flåm, Chief Engineer
Anne-Grethe Kristiansen, Legal Advisor

Norwegian Industrial Security Organisation (NSR)

Rasmus Woxholt, Director of Norwegian Security Council

Norwegian Research Council

Morten Ween, Senior Advisor

Post and Telecom Authority (NPT)

Asle Fuhr, Head of Section
Kari Anne Lang-Ree, Senior Advisor
Tom Opperud, Senior Advisor

Statnett

Tor Aalborg, Senior Consultant Corporate ICT Security
Trygve Kierulf, Head of ICT Division

Tax Directorate

Anders Øksne, Advisor

Telenor

Anne Reinsnes, Security Manager
Erik Wisløff, R&D, Risk Analysis

Annex 7: Members of the Steering Group

DENMARK:

Niels Jacobsen
Head of Section
Danish Emergency Management Agency

Dorte Juul Munch
Head of Section
Civil Sector Preparedness Division
Danish Emergency Management Agency

Niels Madsen
Senior Advisor
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:

Donato Di Matteo
Head of Division for Industrial Risks
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

Alicia Mignone
Science Attaché
Permanent Delegation of Italy to the OECD

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

Francesco Tornatore
Basin Authority of Po river

JAPAN:

Hideki Hirai
Counsellor For Disaster Management
Cabinet Office

Yoshiyuki Imamura
Programme Specialist,
Division of Water Sciences, UNESCO

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

Kotaro Nagasawa
Director of Europe Office
Infrastructure Development Institute

Takashi Nakajima
Deputy- director of Europe Office
Infrastructure Development Institute

Kazuo Umeda
Director of 2nd Research Department
Infrastructure Development Institute

NORWAY:

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

Terje-Olav Austerheim
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

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

SWEDEN:

Ulf Bjurman
Head of Department/Director
Swedish Rescue Services Agency

Oskar Hansson
Principal Administrative Officer
Swedish Emergency Management Agency

Maria Monahov
Research Co-ordinator
Swedish Emergency Management Agency

Alf Rosberg
Project Leader
Swedish Rescue Services Agency

Jim Sandkvist
Director
SSPA

Louise Simonsson
Research Co-ordinator
Swedish Emergency Management Agency

SWITZERLAND:

Rudolf A. Müller
Conseiller scientifique
Secrétariat d’Etat à l’économie

USA:

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

OECD PUBLICATIONS, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(03 2006 02 1 P) ISBN 92-64-02550-2 – No. 55085 2006

OECD Reviews of Risk Management Policies

Norway

INFORMATION SECURITY

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. Cyber-crime has considerably evolved over the years to become a real threat to society. Attack tools have become much more sophisticated, new technologies have brought new vulnerabilities, and critical infrastructures have become dependent on the security of information systems and networks.

Determining the role governments have to play in order to tackle cyber-criminality, reduce vulnerabilities and 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 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. Government policies, therefore, have to be carefully crafted and take advantage of the substantial body of national and international initiatives undertaken in past years.

The review builds on this experience in order to identify areas of good practice among Norway's policies for information security, as well as areas where improvements could be made. With respect to the latter, it proposes opportunities for action and, when possible, suggests alternatives.

This is the first country review conducted in the framework of the OECD Futures Project on Risk Management Policies.

www.oecd.org

9 789264 025509

ISBN 92-64-02550-2
03 2006 02 1 P

OECD
OECDPUBLISHING