

**The investigation into the authorities'
work to secure IT infrastructure
(2005–2006)**

1 Introduction

The technological progress in computer and information systems has given us opportunities to solve a number of societal tasks in new ways. It has also helped to enhance the efficiency of both the public and private sectors. The Vulnerability Commission's report, Official Norwegian Report NOU 2000:24 *A vulnerable society*, states that IT systems have become one of society's cornerstones. This means that society has become vulnerable to failure in these systems. The Vulnerability Commission points out that all IT systems are in constant danger of being attacked, and that the tendency is for more and more enterprises to experience IT-related financial losses. The Hidden Figures Survey showed, for example, that in 2003 around 60% of Norwegian enterprises were affected by computer crime or other unwanted incidents, and that this cost Norwegian enterprises more than NOK 5 billion.¹

In some cases, a failure in IT systems due to random errors has caused considerable problems for those affected, for example when banking systems or a telephone network has been inaccessible to users. These incidents illustrate the potential problems that society may face if anyone should wish to attack important societal functions. The Vulnerability Commission assumes that other states and terrorist groups can, using relatively simple means, paralyse important enterprises and societal functions via hostile information operations.

The Vulnerability Commission's work was an important basis for the government's work as regards civil protection highlighted in Report no. 17 to the Storting (2001-2002) *Samfunnssikkerhet (Civil Protection. The road to a less vulnerable society)*, cf. Recommendation no. 9 to the Storting (2002–2003). Here the government indicates to the Storting that it will also take the initiative to prepare a national strategy for information security. As a result of the report a National Strategy for Information Security was published in June 2003. The strategy has been an important basis for the government's work with IT security over the past few years.

The objective of the report from the OAG of Norway was to evaluate whether the authorities' work on IT security in society was in accordance with the Storting's decisions and assumptions. This involved assessing:

- the way in which the authorities' work is organised
- the measures which have been implemented in this area
- the planning and implementation processes

2 The investigation

The investigation has been conducted by analysing key documents in the public administration's work on information security, through interviews and through a survey.

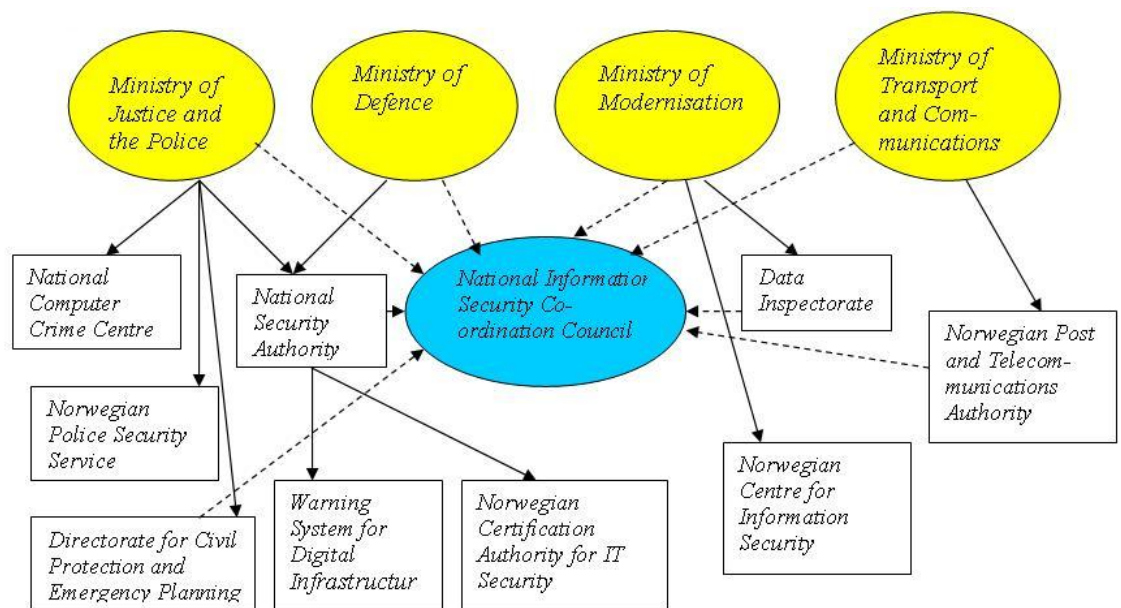
¹ Mørketalundersøkelsen (*The Hidden Figures Survey 2003. Regarding computer crime and IT security*). The National Authority for the Investigation and Prosecution of Economic and Environmental Crime in Norway, the Industry Security Council and the Norwegian Centre for Information Security (NorSIS). June 2004

2.1 The way in which the public administration's work on IT security is organised

Report no. 17 to the Storting (2001–2002) *Samfunnssikkerhet (Civil Protection)* assumes that each enterprise is responsible for its own IT security. The individual ministry is responsible for IT security being safeguarded in the ministry, in its underlying enterprises and within its own sector.

In addition, a number of ministries, government agencies and committees have been assigned coordination tasks and cross-boundary supervisory tasks relating to IT security, as shown in the figure below.

Bodies with key IT security tasks



The figure shows that the responsibility for IT security is divided between a number of ministries and government agencies. While the figure may be complex, it only includes ministries and agencies with central roles, and consequently could have been made even more complex. The ministries are marked with yellow circles in the figure. Their areas of responsibility are discussed in the next paragraph. Subordinate agencies are presented in the white boxes, while the National Information Security Co-ordination Council is represented in blue.² The role of the Council is discussed in more detail below.

The Ministry of Justice and the Police is responsible for coordinating and supervising society's civilian security work and for the emergency preparedness measures in critical infrastructure. The Ministry of Defence is responsible for formulating and implementing Norway's security and defence policy. The Ministry of Modernisation is responsible for coordinating the government's IT policy, including the work on IT

² The solid lines in the figure represent the formal lines of responsibility. Dotted lines represent coordinational functions.

security.³ This ministry is to identify and follow-up issues which affect several sectors, and to initiate and coordinate measures of a cross-sectoral nature in this area. The Ministry of Transport and Communications is responsible for telecommunications security and emergency preparedness, and administers the regulations issued pursuant to the Electronic Communications Act (the Ecom Act), which stipulates requirements as to security and emergency preparedness.

Findings at Ministerial level

Report no. 17 to the Storting (2001–2002) Samfunnssikkerhet (*Civil Protection*) and Recommendation no. 9 to the Storting (2002–2003) point out the importance of coordination and a clarification of responsibilities in the field of IT security work. The investigation shows that clarifications of the ministries' responsibilities are still lacking in the following areas:

- *The responsibility for critical infrastructure*: It is unclear what the Ministry of Justice and the Police's responsibility for critical infrastructure involves, what the responsibility for IT security in this structure involves, and what overall responsibility the Ministry of Justice and the Police has for IT security in an emergency situation.
- *The responsibility for Internet security*: The Ministry of Transport and Communications is responsible for factors which are governed by the Ecom Act, including the Internet, while the Ministry of Modernisation is responsible for the government's overall IT security work. The two ministries' have different views regarding the demarcation between the areas of their responsibilities.
- *Contact with industry*: The ministries were reorganised in 2004. Whether the Ministry of Modernisation or the Ministry of Trade and Industry was to follow up the use of IT in industry was not clarified until April 2005.

The investigation asks what consequences the lack of clarification of responsibilities may have in an emergency situation.

Findings at other professional bodies

The figure above shows that many professional bodies are responsible for tasks relating to IT security. According to among others the government's Report no. 17 to the Storting (2001–2002) Samfunnssikkerhet (*Civil Protection*), the division of responsibilities between various professional bodies must be clarified. The investigation shows that some formal clarifications have taken place between these bodies over the past few years. Most of the professional bodies and trade organisations that are included in the investigation believe, however, that the responsibility for information security in the public administration system is spread over a number of different players, several of which have relatively limited resources in this area. Several of the professional bodies and trade organisations point out that there is fragmentation, a lack of clarification, and that limited resources are used on

³ After a recent reorganization of the ministries this responsibility have now been moved to the Ministry of Government Administration and Reform

overlapping tasks. The trade organisations believe it is difficult to find out which body is responsible for which issues in the field of IT security.

As a follow-up to the National Strategy for Information Security, the National Information Security Coordination Council (KIS) was established in 2004 to ensure that this work was coordinated. The Ministry of Modernisation chairs this committee, which consists of representatives of the ministries and government agencies shown with a dotted line in the figure, as well as representatives of some other ministries and government agencies. The committee has no authority to make decisions, but is to function as an arena for discussion and be an advisory body for ministries and government agencies.

2.2 IT infrastructure that is critical for society

Over the past few decades, IT systems have become an important part of most societal functions, such as the banking and finance systems, electricity and water supply, traffic control systems and systems in the health and social welfare sector. In order to improve the efficiency of the work, the IT systems have increasingly been linked, both within enterprises and across organisational boundaries. This has increased the mutual dependency of IT systems and enterprises, and made it more important to define which parts of the IT infrastructure are critical for society.

A lack of demarcation regarding the IT infrastructure that is critical for society

According to Recommendation no. 9 to the Storting (2002–2003), it is crucial that a robust infrastructure is developed in all institutions that are important to society. This is followed up in the National Strategy for Information Security, in which the protection of critical infrastructure is one of four main goals. According to the strategy, the identification of critical IT infrastructure is a prerequisite for conducting risk assessments and implementing necessary measures. The investigation shows that some work has been started to define critical infrastructure, but that the authorities do not yet have a clear overview of what critical IT infrastructure is and which systems it consists of.

The development of knowledge regarding the IT infrastructure's vulnerability

In Recommendation no. 9 to the Storting (2002–2003), the Standing Committees on Defence and Justice state that the basic knowledge of what creates vulnerability should be given priority in the security work. A research project was established as an important measure for acquiring more knowledge of the vulnerability in nationally important IT systems. The investigation shows that, although this project is referred to as important by both the ministries and other government agencies, it took more than two years to obtain financing and start up the project after it was first mentioned in the draft National Budget in the autumn of 2002. According to the National Strategy for Information Security, norms are to be prepared for each sector in order to protect critical IT infrastructure. The review shows that no activities have been planned or carried out in this area.

The investigation shows that most of the public bodies working on IT security have prepared guides for conducting risk and vulnerability analyses, and many activities are being carried out to further develop methods and tools. However, the authorities have to a lesser extent placed emphasis on making arrangements for these methods to

actually be used. Nor have any arrangements been made to enable the use of knowledge obtained from the analyses when prioritising security measures.

Systems for identifying threats

Information on security incidents is necessary in order to obtain a picture of the threats and vulnerability in the IT infrastructure, and in order to provide advice on concrete threats or assistance in restoring services. The Warning System for Digital Infrastructures (VDI) and Norwegian Centre for Information Security (NorSIS) have been established for this reason.

The investigation shows that the Warning System for Digital Infrastructures has succeeded in gaining access to information on logical threats via the Internet. Report no. 17 to the Storting (2001–2002) Samfunnssikkerhet (*Civil Protection*) points out that this system is also to be as open as possible regarding who can be a participant and user, and that the information is to be as accessible as possible. The investigation shows that the system has a limited number of participants and that information to the general public is limited to a brief monthly summary of registered incidents.

According to Parliamentary Bill no. 1 (2001–2002) for the Ministry of Trade and Industry, NorSIS is to contribute to a more robust IT infrastructure by, among other things, providing an overall picture of the threats to Norwegian IT systems. This is to take place by public and private enterprises reporting security incidents to this body. According to the Mørketallsundersøkelsen (*Hidden Figures Survey*), Norwegian enterprises were subject to around 5,200 computer break-in incidents and 2.7 million attempted computer break-ins in 2003.⁴ In 2004, fewer than five security incidents were reported to NorSIS.

By establishing the Warning System for Digital Infrastructures and NorSIS, the authorities have created bodies that can identify threats to IT systems, but these bodies have so far not achieved any of the important goals for their activities. The investigation therefore questions whether the ministries have decided on sufficient measures to ensure goal achievement in this area.

Ability to deal with security incidents

The Standing Committees on Defence and Justice in the Storting stated when concluding on Report no. 17 (2001–2002) Samfunnssikkerhet (*Civil Protection*), that it is important to clarify emergency preparedness plans and emergency response plans for such areas as IT security. The Report to the Storting states that the Ministry of Justice will take the initiative to ensure that measures to cope with the failure of IT are reflected in emergency plans.

The investigation shows that only a minority of the enterprises in the state, municipal and private sectors have up-to-date emergency preparedness plans. The National Strategy for Information Security does not contain any measures that are directly aimed at promoting the development of good emergency preparedness and

⁴ Mørketallsundersøkelsen (*The Hidden Figures Survey 2003. Regarding computer crime and IT security*). The National Authority for the Investigation and Prosecution of Economic and Environmental Crime in Norway, the Industry Security Council and Norwegian Centre for Information Security (NorSIS). Pages 20–24

emergency response plans. The investigation asks whether the lack of emergency preparedness plans in these enterprises may involve a risk to society.

In Recommendation no. 9 to the Storting (2002–2003), the Standing Committees on Defence and Justice point out that it is important to carry out training exercises in order to obtain a management that can deal with emergencies. These committees also state that employees dealing with security, emergency preparedness and emergency response should be treated as a target group for these exercises on a par with the management level. The review shows that training exercises initiated by the Directorate for Civil Protection and Emergency Planning (DSB) have to a large extent concentrated on the management level, while subordinate employees seem to have been given lower priority. The OAG therefore asks whether the training exercises system has complied with the assumptions of the Storting.

The OECD Guidelines for the Security of Information Systems and Networks places emphasis on the importance of having systems that can prevent, discover and react to security incidents. Many countries have therefore established a state-financed CERT.⁵ Report no. 39 to the Storting (2003–2004) *Samfunnssikkerhet og sivil-militært samarbeid (Civil Protection and civilian-military cooperation)* refers to the fact that several bodies have pointed out the need for such an entity (CERT) to ensure the efficient handling of emergencies in which several functions that are critical for society are attacked simultaneously. According to the Report to the Storting, such an entity will be able to strengthen the national emergency preparedness for IT attacks by developing a system for coordinated response and restoration, primarily in enterprises that carry out functions which are critical for society. The investigation indicates that there is agreement that a CERT should be established but disagreement regarding which professional environment is to be assigned this task. No system that can efficiently deal with IT security incidents has yet been established.

2.3 Arrangements for the development of a good culture of security

The development of a good culture of security is the basis of the OECD Guidelines for the Security of Information Systems and Networks on which the ministries have based their work in this area. The National Strategy for Information Security contains a number of measures intended to contribute to the development of such a culture. These measures are primarily linked to the development of general IT security. They will influence the security level of the IT infrastructure that is critical for society, but the measures are also aimed at companies and households.

The investigation shows that few new measures to develop a good culture of security have been implemented or initiated. The nettvett.no Internet portal has been established, but the other planned measures for making the general public aware of IT security have not been initiated and there are no specific plans for implementing them. The private organisations that are included in the investigation do not consider the public sector to be a driving force or a good example for the private sector's work on IT security.

⁵ CERT stands for Computer Emergency Response Team and is a group of experts who deal with IT security incidents.

The feedback from trade organisations indicates that the authorities' work of developing a culture of security has so far not been of significance to the private sector. The investigation therefore asks whether the authorities' efforts have been sufficient.

3 Possible reasons for the lack of progress in the IT security work

The investigation shows that there are various reasons for the lack of progress in the IT security work and in the implementation of measures stated in the National Strategy for Information Security. The lack of a clarification of the division of responsibilities is stated to be a possible reason, cf. item 2.1. In addition, the following factors are pointed out:

Limited participation in the implementation of measures

The National Strategy for Information Security makes selected trade organisations co-responsible for implementing a number of measures. As at May 2005, the ministries have not contacted the selected organisations regarding the implementation of these measures. Measures in the school and university sector are also delayed and no sufficient collaboration has been established between the Ministry of Modernisation and the Ministry of Education and Research.

Insufficient planning documents

The most affected ministries have prepared plans of action for following up the National Strategy for Information Security. However, these plans are to a large extent summaries of what is done within each ministry's area and are in many ways no more detailed than the strategy. The plans of action contain little prioritisation of measures or information on how the measures are to be achieved, ie, a link to estimated resources and budgets.

Lack of formal authority

The way in which the public IT security work has been organised and the National Strategy has been formulated does not impose any obligation on the individual enterprise to implement the measures in the strategy. With this as a starting point and with so many enterprises involved in implementing the strategy's measures, it is a difficult task to monitor that the strategy is realised effectively. The investigation shows that the Ministry of Modernisation, which is responsible for coordination within this area, has few IT security-related instruments and has set aside relatively limited resources for this activity.

A lack of coordination of the regulations

The National Strategy for Information Security emphasises that the IT security regulations are to be better coordinated. In the investigation report, several government agencies and trade organisations point to factors in the regulations that may make the coordination of the security work difficult. The complexity and fragmentation of the regulations is stated to be a problem for industry/the users. The investigation shows that it took just over 18 months from the date when the strategy was presented until a pre-project was established to review the regulations. Several

attempts have previously been made to achieve such a coordination without these having the desired effect.

4 Concluding remarks

The Office of the Auditor General's investigation shows that the authorities' work on IT security is characterised by having many players and an unclear division of responsibilities. The Office of the Auditor General wishes to emphasise the importance of the affected ministries coordinating this work to a greater extent. The Office of the Auditor General has noted that the Ministry of Modernisation appointed an interministerial workgroup in October 2005 to assess the division of responsibilities in further detail.

IT infrastructure that is critical for society is characterised by a strong mutual dependence between systems and between sectors. The infrastructure is also increasingly exposed to threats. In the Office of the Auditor General's opinion, it is now important to clarify which authority is responsible for obtaining overviews of the vulnerability in critical infrastructure across sectoral boundaries and for coordinating measures to reduce the level of vulnerability.

The Office of the Auditor General has noted that an integrated concept for national warning and advice relating to IT security is to be established, based on the creation of a national CERT (Computer Emergency Response Team) and the re-establishment of the Norwegian Centre for Information Security (NorSIS). The Office of the Auditor General wishes to underline the need for clear limits of responsibility and good forms of cooperation between CERT, the Norwegian Centre for Information Security (NorSIS) and other public bodies that are working on IT security. The Office of the Auditor General also wishes to point out the importance of the handling of serious failures in IT systems being reflected in emergency preparedness plans at various levels, including in a new national emergency preparedness system.

The Office of the Auditor General's investigation also shows that the ministries' plans of action for following up the National Strategy for Information Security only to a slight extent contain any prioritisation of measures or state when and how measures are to be implemented. No performance requirements have been stipulated to enable the effect of the measures to be assessed. The investigation also shows that the responsibility for IT security seems to be too poorly coordinated and suffers from a lack of integrated management and follow-up. The Office of the Auditor General wishes to underline the importance of the public protection against IT attacks being given highest priority and of emphasis being placed on a coordinated, integrated management and follow-up of the work on IT security.