

The Swedish National Audit Office

IT Security at the National Tax Board

Report No. No 1999:23

RRV Publication Service, Telefax no 46-8-6904100, E-mail: publikationsservice@rrv.se

SUMMARY:

The RRV has studied IT security at the National Tax Board. The Board is responsible for several important computer systems which contain sensitive information involving the integrity of individual persons and companies. The systems also handle a considerable amount of money. For these reasons there are strict requirements in respect of IT security at the National Tax Board. The need to make the systems secure is further underlined by the fact that electronic communication with tax payers will increase in the future.

The starting point of the audit has been to shed light on the problems which can arise in a government agency's computer systems and on the capacity of the agency to deal with matters relating to security. This report describes and assesses the work done by the National Tax Board on security, particularly in respect of organisational issues, administrative routines, training of personnel, and technical solutions of potential security problems.

The National Tax Board is the parent agency of a group with 14,000 employees. A special profit centre in the agency, Data Service, is responsible for IT services.

The level of security has been overestimated

At the National Tax Board, levels of IT security are considered to be high. However, the RRV's study shows that a number of incidents have occurred during recent years: computer viruses, embezzlement, thefts of information and thefts of computers. Furthermore the National Tax Board has been used as a relay for sending electronic post with a false sender, and a stolen portable computer has been used in an attempt to ring up the internal network.

Most of these events have not caused extensive harm or damage. But information on these occurrences has only been spread to a small number of persons in the agency. This situation may have contributed to the impression of the high level of security.

The main emphasis of the National Tax Board's work on computer security has been on technical solutions, and it is in this area that considerable investments have been made. On the other hand the investments made by the agency in developing administrative routines for IT security and in the training of staff have been comparatively small. In the opinion of the RRV, this has had the effect that the value of the technical solutions, and thereby of overall IT security, is lower than intended. Furthermore there are deficiencies in technical security and in the use of installations for technical security. In the light of this situation the RRV considers that the National Tax Board has overestimated the level of its IT security.

The organisation of IT security work is not clearly defined

A specific division of responsibilities is a prerequisite for success in working with IT security. However, the RRV's study shows that the division of responsibilities at the National Tax Board is blurred. One example of this is that there are varying opinions on who owns the systems and who actually places orders in respect of IT security.

The Swedish National Audit Office

IT Security at the National Tax Board

At the National Tax Board a small number of people are responsible for important parts of the work on IT security. There are systems which can only be operated and maintained by just a few members of staff.

There are deficiencies in the administrative routines for IT security

Administrative routines in this context refers to the rules and analyses which supplement the technical solutions. One important part of the administrative routines is the National Tax Board's IT security policy. However this has not been updated since 1993, which may have contributed to the fact that the policy has only been used to a small extent in the practical work on IT security. The National Tax Board also lacks directives which stipulate levels of security in detail.

Risk analyses can provide information on threats to IT security. Analyses of this type also make it possible to evaluate the extent to which requirements and guidelines are observed and the level of security which actually exists. Risk analyses are only made at the National Tax Board when new systems are introduced. In the opinion of the RRV this is not sufficient since threats to security can change form.

Effective monitoring of the improper use of computers and of computer crimes provides information - and time to take counter measures. Information on incidents which is collected in a reporting system can constitute the basis for decisions on detecting and reporting incidents to the police. However today the National Tax Board does not have a reporting system of this type.

At the National Tax Board the staff rely to a great extent on the system for access control in their security work. However the National Tax Board's internal audit has shown that the employees' access to IT support is often higher than necessary for the performance of their duties.

Not enough training and too little information

At the National Tax Board there is no regular training in IT security despite the fact that this is stipulated in a security handbook.

Neither is there any regular further training of staff at Data Service in technical IT security matters. One consequence of this can be that there is a lack of knowledge of the technical security products that are available on the market. As an example of the problems that can arise, mention can be made of the fact that the Data Service has installed a technical modern firewall in an out-of-date way. The firewall thus provides less protection than it could provide.

The technical solutions still suffer from deficiencies

As many other organisations, the volume of external electronic communications at the National Tax Board has increased. This creates demands in respect of detecting and combating viruses. However the National Tax Board lacks routines to update its virus program. One explanation of this can be that the National Tax Board has not yet experienced any serious problems from virus attacks.

Logging has the purpose of making investigations possible of any important events which have taken place in a system. At the National Tax Board there are no routines for the manual control of logs. Likewise there are no automatic tools for linking and matching and making comparisons of logs in and between systems. At present logs are only analysed randomly, when the systems administrators have the time to do so. Therefore there is no complete picture of trends, patterns and

The Swedish National Audit Office

IT Security at the National Tax Board

contexts which can provide information on deviations and problems in the systems. There is a danger that incidents can pass undetected. A further problem with the logs is they can be manipulated relatively easily in the form they are stored at present. Therefore their authenticity can be questioned and it can be difficult to use them as evidence in a criminal investigation.

At the National Tax Board logging in with the use of terminals and smart cards is considered to be technically secure. However the computers which are used for the development of software do not have this form of protection. These computers can be used as a springboard to reach production systems and to obtain source codes and other valuable information which can then be stolen or manipulated.

The RRV's proposals to the National Tax Board

The work on IT security should be an ongoing process. This means that issues relating to organisation, administrative routines, training and technology should be given continuous attention. Therefore, if the work is not to come to a standstill, recurrent controls and examinations are necessary. It is also important that a balance is achieved between the costs of the work on IT security and the advantages provided in the form of reduced risks which the IT security work is intended to give.

Organisation

In order to create a better organisation for its work on IT security, the National Tax Board should:

- further define the division of responsibilities in the work on IT security
- analyse and reduce dependence on key persons
limit the possibilities of persons working from home to obtain access to operational data

Administrative routines

To benefit more from its investments in technical security systems, the National Tax Board should develop its administrative routines by:

- updating and creating directives for the implementation of the IT security policy
- making emergency plans for all important systems
- starting, as soon as possible, work on ensuring that levels of access to systems match working duties
- introducing routines for the implementation of risk analyses, security checks of personnel, incident reports, and the elimination of old user accounts.

Training and information

For reasons of continuity and spreading information on the work on IT security, the National Tax Board should:

- regularly train, inform and motivate the staff in matters concerning IT security,
- give the staff at Data Service continuous further training to maintain their technical expertise in the area of IT security,
- develop routines to ensure that the agency is kept up-to-date in respect of threats which can affect operations.

The Swedish National Audit Office

IT Security at the National Tax Board

Technical security systems

To further improve its technical security solutions the National Tax Board should:

- implement code checks as part of the development work,
- introduce regular mechanical security reviews and controls of all systems and investigate the consequences of having reactive security control programs,
- consider the measures which should be taken to minimise the security risks associated with the sensitive server for access control,
- change passwords regularly in all systems,
- devise uniform and reliable logging routines and select a secure method for time synchronisation in the systems,
- reinforce the fire-wall environment in Data Service and the protection against viruses.

Head of section (contact person):

Rutger Banefelt
+46 8 690 4181
e-mail:rutger.banefelt@rrv.se

Project manager:

Charlotta von Porat
+46 8 690 4417
e-mail:charlotta.vonporat@rrv.se