SWEDISH NATIONAL
AUDIT OFFICE

Summary

Date: 2023-04-13
Reference number: 3.1.1-2022-0145
RiR 2022:8

Government control of national information and cyber security

– both urgent and important

Summary

Digitalisation has had an impact in all sectors of society at all levels, leading to a greater need for both information and cyber security. Moreover, the cyber security threat is said to be increasing. The responsibility of managing risks, threats and vulnerabilities and increasing security is shared within the Government Offices as well as among government agencies. The Government's national cyber security strategy outlines a number of objectives for these efforts. Problems still remain in all areas of the strategy, six years after its introduction.

The Swedish National Audit Office (Swedish NAO) has therefore audited whether the Government's efforts to strengthen Sweden's national information and cyber security have been efficient. The Swedish NAO's overall conclusion is that the Government's work in this area has not been efficient. The main shortcoming has been a lack of strategic considerations and priorities to direct cyber security efforts. A clear example of shortcomings in strategic considerations is Sweden's approach to the issues within and in relation to the EU. The work in the EU is high paced and if Sweden is not engaged and influences that work early on, there is a great risk that the international regulatory framework will not favour Swedish interests to the same extent as would otherwise have been possible.

Nor has the Government produced or implemented the national cyber security strategy in accordance with international best practice. According to the Swedish

NAO, the strategy lacks a clear vision, objectives that can be followed up, parties responsible for implementing measures, and resources allocated for the work. In the absence of a clear policy, the ministries and government agencies proceed based on their respective goals and priorities. This makes it difficult to ensure that the implemented efforts are the appropriate ones for Sweden's national information and cyber security, and that the efforts are carried out efficiently. This risks leading, not only to a lack of effect on the part of the implemented measures, but also to an inefficient use of resources.

The Government's control has therefore largely been based on separate issues that have not been valued or ranked on the basis of their benefits to Sweden as a whole. The Government Offices have sought to improve cohesion in their efforts by establishing inter-ministry working groups and tasking a number of agencies with creating a national cyber security centre (NCSC). The assessment of the Swedish NAO is that this has not led to an increased capacity for giving priority to measures based on Sweden's overall needs in the information and cyber security field, or to long-term, strategic, holistic and cohesive governance of the area. According to the Swedish NAO, the shortcomings have led to weak governance in the information and cyber security field on the part of the Government. It has also impeded progress on national information and cyber security efforts.

Exchanging information is an important component for the ability to work towards the same goal and coordinate efforts. The Swedish NAO's assessment is that the exchange of information, both within the public sector and between the public and private sectors, is currently not functioning efficiently. At present, the government agencies produce several different and partially overlapping situational reports, but no report provides an overview. The business sector does not feel that it receives sufficient information from the public sector and is under the impression that the government agencies are not interested in receiving information from them. Other collaboration with the business sector has also been difficult to bring about. For example, the business sector was involved to a limited extent both in the development of the strategy and in the construction of the NCSC. Overall, this risks leading to the Government Offices and the government agencies not gaining a proper understanding of the business sector's needs, what the enterprises can contribute, or a clear status report of the most important risks and threats to Sweden in the cyber environment. The exchange of information is burdened with certain legal, technical and cultural challenges. It is therefore important that the Government Offices and the government agencies find forms for addressing these challenges.

Recommendations

The Swedish NAO makes the following recommendations to the Government:

- Establish a strategic, holistic, and long-term focus for work on information and cyber security. This focus should include an analysis of the national strategic challenges, considerations, and priorities, as well as resource allocation and an action plan for implementation. The work should involve relevant stakeholders.
- Establish concerted governance with clear lines of responsibility, sufficient competence and efficient forms of coordination concerning information and cyber security issues at the Government Offices.
- Identify obstacles to information exchange and ensure that structures are in place that allow necessary information exchange between government agencies as well as between the public and private sectors so that work on national information and cyber security is efficient.
- Review the remit, mandate and organisational designation of the national cyber security centre to secure its contribution to the information security and cyber security of society as a whole.