Swedish Civil Contingencies Agency

Strategy for information security in Sweden

2010 – 2015

Foreword

In today's information society, we process, store, communicate and duplicate information in greater quantities than ever before. Information handling is done manually and, to an increasingly greater extent, with the support of IT – like, for example, the public network that is the Internet.

Information security requires all information to be protected on the basis of confidentiality, integrity and availability requirements. This applies to both individuals and organisations.

In other words, information security is everyone's business.

Information and information management should be of a high quality in Sweden. All stakeholders in society should have relevant knowledge of information security and be able to feel confidence in information and how it is handled at all levels in society.

Information handling shortcomings could lead to confidence in current services and in the stakeholders behind them being reduced. Serious and frequent disruptions could lead to crises of confidence, which could also spread to more stakeholders and services and even to others sectors of society.

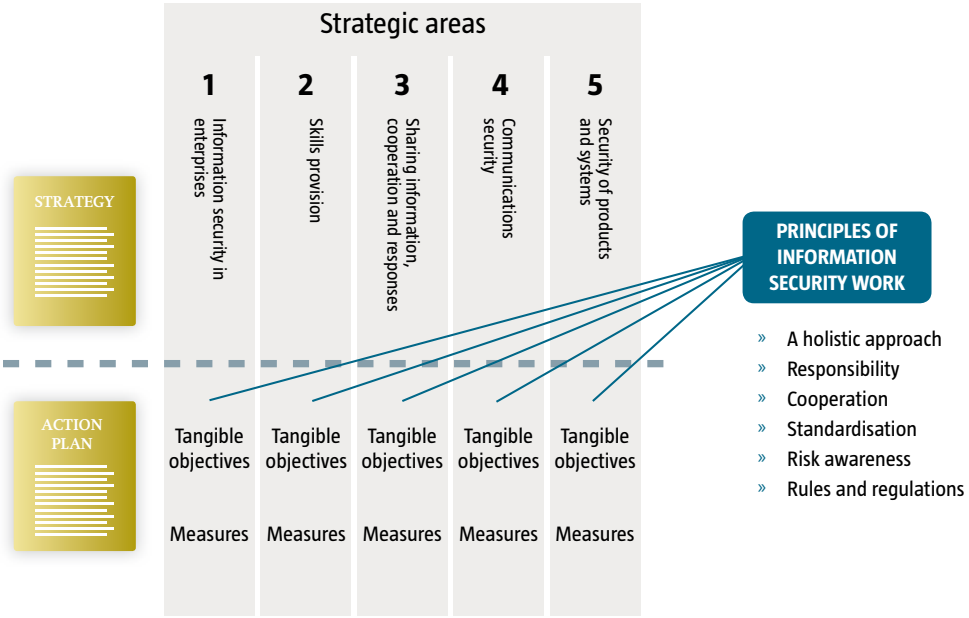
In order to meet the challenges within the information security sector, it is important that there is a common understanding of information security in our society: a strategy.

In these circumstances, the MSB The Swedish Civil Contingencies Agency has, in cooperation with the Swedish Armed Forces, the Swedish Defence Materiel Administration, the Swedish National Defence Radio Establishment and the Swedish Post and Telecom Agency, produced this strategy for societal information security. In addition to this, the Swedish Security Service has provided its points of view on the strategy in question.

Helena Lindberg, Director-General

STRATEGIC OBJECTIVES

- The freedom and rights of citizens and also their personal integrity.
- The functionality, efficiency and quality of society.
- Society's fight against crime.
- Society's capacity to prevent and deal with serious disruptions and crises.
- The growth of the economy.
- Citizens' and enterprises' knowledge of and confidence in information handling and IT systems.



The direction of societal information security

The aim of this strategy is to provide long-term objectives, directions and methods of working for information security in Sweden.

A number of different stakeholders in our society need a common understanding of information security, its purpose and what the focus and form should be for future security initiatives. The primary parties concerned are those working in the area of information security at various levels, decision-makers in public administration and in trade and industry and those working in the area of IT or general security, but also private citizens.

For this reason, the strategy includes our entire society, i.e. all state authorities, municipalities and county councils, companies, organisations and private individuals.

Together with the national action plan, this strategy for societal information security states the direction information security in Sweden is taking.

The strategy indicates strategic objectives, strategic areas and principles for information security work. The objectives are to be achieved by working within the strategic areas in the manner expressed in the principles.

The strategic areas are to be found in the national action plan in the form of chapters that contain tangible objectives and measures.

The strategy will be administered by the MSB. Together with the authorities concerned, the MSB will update the strategy at least every six years.

Information security is a support activity for increasing the quality of societal functions

Strategic objectives

Information security is a support activity for increasing the quality of society's functions. Ultimately, it is about standing up for important values and objectives in our society, such as democracy, personal integrity, growth and economic and political stability.

The extensive use of IT in society means that information security is also a prerequisite for new phenomena in society, such as e-administration, being able to function.

The objective is to achieve a good level of information security in our society so as to promote:

- the freedom and rights of citizens and also their personal integrity
- the functionality, efficiency and quality of society
- society's fight against crime
- society's capacity to prevent and deal with serious disruptions and crises
- the growth of the economy
- citizens' and enterprises' knowledge of and confidence in information handling and IT systems

Strategic areas

1. Information security in enterprises
2. Provision of skills
3. Information sharing, cooperation and responses
4. Communication security
5. Security of products and systems

1. Information security in enterprises

Information handling takes place in all areas of society and societal information security is subsequently dependent on a great number of stakeholders. State authorities, municipalities, county councils and other organisations have different conditions and thereby different needs and information safety requirements.

Enterprises handle information that is more or less confidential and where it is critical that this is correct and accessible. Having a good level of information security is an important internal matter for most enterprises in order to achieve their quality and effectiveness requirements. At the same time, information security cannot be regarded as a domestic matter exclusively for enterprises. The flow of services and products takes place at several levels and a lack of information security could, therefore, have a resulting effect far beyond the boundaries of the individual enterprise.

Information security is about the quality of the enterprise. Improving information security is not just about accommodating external requirements; it also involves actually improving the enterprise. Having a good level of information security should, therefore, be regarded as a quality aspect, a way of achieving good internal control, order and clarity. Good information security is also a prerequisite for a number of IT-based services that could, in themselves, be cost-saving or income-yielding for the enterprise.

2. Provision of skills

Knowledge about the risks involved in IT and electronic communication via, for example, the Internet, must be taught at an early stage and be an integral and natural part of initial IT use. It should then follow on throughout the entire time at school and be included in higher education, particularly as an integral part of courses that lead to professions involving a considerable information handling element.

In many activities, the human factor is critical. Major costs for incidents can be traced to a lack of awareness and skills among management, users and IT personnel. In different activities, different types of knowledge are required in a number of different roles. It is people who develop, install, configure and use technical systems. It is people who formulate, communicate and monitor administrative systems. One particularly important group from an information security perspective is organisation management teams, as they are ultimately responsible for the quality and security of the enterprise and make decisions on protective measures.

An area that is as multi-faceted as information security needs to be studied in greater depth. Research and post-graduate studies are necessary in order to maintain both a general knowledge and a cutting-edge knowhow within the area. National research and post-graduate studies will also improve teaching skills within the area, from comprehensive school to colleges and universities.

3. Information sharing, cooperation and responses

Sharing and disseminating information is important in order to make use of and spread knowledge and experiences within the information security field. Such knowledge and experience is available everywhere in our society, within both the public and private sectors.

For this reason, it is important that there are effective networks within and between the private and public spheres. This is particularly clear when it comes to the critical Swedish information infrastructure that exists in both public and private ownership, and both the public sector and trade and industry may benefit from sharing their experiences.

Our global world with boundless threats also requires international cooperation. Sweden should actively participate in international collaboration on several levels: within the EU, with the Nordic countries and with individual states.

IT-based disruptions and attacks can often spread quickly across organisational boundaries at great speed. Society needs to have a good capacity for preventing these and, if they occur nevertheless, be able to manage these events in a satisfactory manner.

Traditional crime, such as fraud, extortion, defamation and sabotage, can also be found on the Internet today. This is a threat to society and we must counteract these new types of crime.

4. Communication security

Information handling regularly takes place between several stakeholders, which makes great demands on telecommunications and computer networks. For example, the Internet carries a great proportion of our information flow.

In this context, it is important to have robust critical functions in the infrastructure for electronic communications and that there are secure cryptographic functions and signalling protection. For the sharing of confidential information, it is also necessary for electronic services to be based on effective and secure systems.

5. Security of products and systems

The long-term provision of secure IT products makes great demands on formal frameworks for the evaluation and certification of security properties. These frameworks should be nationally and internationally accepted.

Within the area of industrial control systems for enterprises that are of great social importance – e.g. electricity and water distribution, trackbound traffic and the petrochemical industry – IT systems are used to manage and monitor the central physical processes. It is of major importance that these systems have a high level of security.

Principles for information security work

A holistic view

Responsibility

Cooperation

Standardisation

Risk awareness

Rules and regulations

A holistic view

In order for information handling and the use of IT in society to be developed in a safe and secure manner, it is necessary for all stakeholders to take a holistic view of information security. Information security is a complex and cross-border area that also embraces technology, administration, economics and jurisprudence. When we work towards improving information security in organisations and at a national level, we must take account of several perspectives.

Information security should be an obvious and integral part of all IT and information-related work at all levels in society; within and between organisations and within and between society's different sectors.

Security measures should aim to both create more robust information handling during times of normality in society and also to handle more serious disruptions and crises. Effective everyday security is often on a par with being prepared for serious incidents. For example, good internal control in enterprises, good information security skills and sharing information with others gives a reassuring ability to handle a crisis.

Responsibility

All work in the area of information security should be based on the regulated responsibility in society, such as the principle of responsibility. This states that "An entity who is responsible for an activity under normal conditions should have the corresponding responsibility in the event of a crisis or war scenario."

Responsibility for information security normally follows the responsibility for the activity and should be unambiguous. In order to conduct successful information security work, it must be clear who has responsibility for what. This applies at all levels – both within organisations and in society in general.

Cooperation

The complexity of information security, its cross-border nature and rapid rate of development require effective cooperation. Good cooperation in the area of information security in society is important under normal conditions, but also a necessity if we are to create a good operational capacity for handling serious disruptions. This involves cooperation between different stakeholders in Sweden, such as state authorities, municipalities and county councils, trade and industry and interest groups, but also international cooperation.

Sweden should be active both in the EU and internationally, for example in technology research and development, and be involved in the formulation of rules and regulations and other means of control. In addition to cooperation within the EU, cooperation with a number of other countries is also necessary, for example the Nordic countries

Standardisation

Standards that support information security should be applied, as they are based on experience and make the most of existing achievements. In this way, a higher level of security can be attained and unnecessary mistakes avoided. Standardisation simplifies training and therefore also improves skills. Standards also increase transparency between organisations, which makes it easier to make demands and assess products, systems and entire enterprises.

Risk awareness

Resources are required in order to be able to attain secure and safe information handling in society. Security aspects should not be regarded as an additional cost item, but as an obvious investment in order to achieve the intended functionality and quality.

Investments for building in and improving security should always be compared with what it could cost not to do so. The objective is to find the correct level of security and for those responsible to be aware of the risks that exist so that they can actively make decisions to eliminate, reduce or accept these risks. This kind of risk awareness will form the basis for effective information security investments.

Investments in information handling are frequently carried out for the purpose of streamlining and rationalising services in society. It is, therefore, reasonable to invest some of these savings in achieving quality and robustness through an increase in security initiatives.

Rules and regulations

A prerequisite for a good level of information security in society is the existence of regulations in line with modern information handling. This applies at both enterprise and society level. Rules and regulations should be clear, communicable and, if possible, dependent on technology so that they are effective over time. Nor should they restrict competitiveness.

ADVANT PRODUKTIONSBYRÅ

MSB points of contact:

Richard Oehme
E-mail: richard.oehme@msb.se

Wiggo Öberg
E-mail: wiggo.oberg@msb.se

Swedish Civil Contingencies Agency (MSB)
651 81 Karlstad Tel. +46 (0)771-240 240 www.msb.se/en
Publ.nr MSB243 March 2011 ISBN 978-91-7383-126-0