Swedish Civil Contingencies Agency

Information security in Sweden

Situational assessment 2009

Contact person at Swedish Civil Contingencies Agency (MSB):
Helena Andersson, tel +46 10 240 41 33

Publication nr: MSB 0119-09
ISBN 978-91-7383-053-9

Preface

The Swedish Civil Contingencies Agency's (MSB) remit is to support and coordinate the work on societal information security as well as to analyse and assess outside developments in this field. There is a target-oriented work going on within the society in order to promote the use and availability of electronic services. Confidentiality and user friendliness are decisive factors of success, but inadequate technical solutions, incomplete protection of integrity and insufficient security awareness create obstacles for an efficient use of IT.

This situational assessment is a part of the surrounding world coverage and analytic work pursued at MSB within the field of information security.

The situational assessment is primarily build on information from 2008 and the beginning of 2009 and is intended for actors in society managing issues concerning information security.

Stockholm March 2009

Helena Lindberg

Director General

Table of content

Summary

Societal functions are dependent on functioning IT and information management, thus a sufficient level of information security is a necessity. The weak link in the security work is human behaviour, which can both hamper protection of information management and constitute direct threats to it. The threats are becoming increasingly sophisticated, and cybercrime is being committed in a business-like way. Crime-fighting is being restricted by a lack of resources, and the judicial system is suffering from a shortage of skilled staff regarding IT related evidence.

A more and more complex IT environment and increasingly integrated networks mean that the emphasis is often on more restricted and manageable IT related problems in one's own organisation. It is important to also draw attention to and analyse consequences and connections from a societal perspective. What happens if the large majority of organisations with societally critical functions outsource their information management to foreign companies?

The field of information security has long been characterised by the lack of a holistic approach and control. There are currently several plans of action that are of crucial significance to the security work, and the Swedish Civil Contingencies Agency (MSB) has a regulatory right regarding authorities' information security. Appropriate work on information security at national and international level is of crucial significance to societal development.

Target-oriented work is taking place on increasing use of and access to electronic services in society. Confidence and user-friendliness are crucial success factors, but inadequate technical solutions, incomplete protection of integrity and insufficient awareness of security create obstacles to efficient utilisation of IT. It is thus important to emphasise the importance of appropriate work on information security to deal with these deficiencies.

The rules governing work on information security were changed in 2008 in the form of new technology, new regulations and new user behaviours. Outsourcing in the form of Cloud Computing will allow organisations to concentrate on their core business, but will simultaneously entail less control of information management. Increased mobility and greater use of interactive social networks mean higher risks for both organisations and individuals, as the issue of security is not yet a major user requirement. Security work is being neglected in the field of website development and operation. As visitor numbers increase and threats become more serious, this may in the long term damage confidence in both the content and management of personal data.

The threat is becoming more serious, and cybercrime is already a significant problem. In this context we are witnessing increasingly sophisticated fraud that is increasingly exploiting human weaknesses. Various forms of blackmail constitute an area that has proven hard to combat and in which a large number

of unrecorded cases is feared. Criminal circles are adopting a very businesslike approach – something that is demonstrated by an established trade in attack tools, experts and renting-out of hijacked computers. The Swedish Emergency Management Agency (SEMA) highlighted this development back in 2007, and it became more marked during 2008.

The crime-fighting is encountering challenges in the form of unrecorded cases and a lack of resources concerning cybercrime. The shortage of staff in the judicial system when it comes to production of IT-related evidence also has to be dealt with. International and national cooperation is a prerequisite, not only for implementation of efficient work against cybercrime but also so as to guarantee national security.

There are currently plans of action for societal information security, security of internet infrastructure and e-government, and several independent initiatives to create information security. With regard to the steadily increasing dependence on IT and the development of threats and vulnerabilities, we consider it crucial that proposed measures such as skills enhancement and establishment of basic information security be implemented. There should be further measures to counteract cybercrime and promote international collaboration.

List of terms and abbreviations

Botnet – Network of computers infected with malicious code that allows a third party to control computers and operate them remotely.

Buffer overflow – Exceeding a maximum permissible quantity of data in the memory buffer, which can result in destruction of or damage to the system.

CERT (Computer Emergency Response Team) – Incident-management function

CCRA (Common Criteria Recognition Arrangement) – An international collaborative organisation that recognises mutually issued certificates. Within the parameters of the CCRA both methods and regulatory frameworks to support the CCRA agreement and the Common Criteria standard are being developed.

Common Criteria – An international standard for issuing of requirements, declarations and evaluation of security in IT products and systems.

Communities – Websites for which sharing of content often requires membership. The main aim is usually to come into contact with like-minded people.

COTS (Commercial Off-The-Shelf) – Commercially available standard products.

Cross-site scripting – Method that exploits the user's confidence in an internet application. The aim for an attacker is usually to steal sensitive information such as a password or to destroy the appearance of a website. Links to other websites can also be posted on the site.

DDoS (Distributed Denial of Service) attacks – Activities that may overload or block certain IT resources and thus prevent authorised access to resources in an IT system or delay time-critical operations.

Digital control systems (SCADA – Supervisory Control And Data Acquisition) – Computer-based systems for control, regulation and monitoring of physical processes such as electricity, gas, track-bound traffic and provision of drinking water.

DNS (Domain Name System) – The function on the internet that translates domain names into IP addresses. As there are many domain names, and as no individual server can have a complete list of them, there is instead a network of interconnected DNS servers that ask each other for help when necessary.

Drive-by downloads – Programs that are downloaded to the computer without the user's knowledge or consent. Such downloads can result from simply visiting a website. The reason for computer infection is often a poorly updated web browser.

Exploit – Method used to exploit vulnerability in a computer system so as to access protected information or for the purpose of sabotage

Hosting – Instead of buying, installing and operating servers and software locally for every PC, a company can gain access to IT services and applications over the internet and pay for a specific period. An external hosting provider then supplies various solutions.

Man-in-the-middle attack – Outsider who by linking to a connection between two parties shows a simulated identity for one party to the other party, and who can thus intercept or change the information transferred.

Metasploit – Hacking tool that allows both system administrators and hackers wishing to perform a penetration test to combine attack code for a number of different security holes with other malicious code

Phishing (internet fishing) – Method that seeks to get people to disclose confidential information by tricking them into either replying to a false e-mail or visiting a false website.

OpenID – Solution that means that once an OpenID provider has been accessed, only a single log-in by means of user name and password is necessary. The provider then assures the user's identity for other internet applications that require log-in.

PGP (Pretty Good Privacy) – PGP is based on a system of private and public keys. Anyone wishing to send someone an encrypted message uses that person's public key. The recipient then uses his private key to decrypt the message.

RAKEL (RadioKommunikation för Effektiv Ledning = Swedish Public Safety Radio Communication System) – Common radio communication system for societal organisations working in the field of general order, security or health.

Remote file inclusion – Type of attack in internet-based written language. The attack means that a person can execute their own written code on someone else's server. It is then possible for an attacker to gain access to all the files on the website and change them if the rights are not correctly set on the internet server.

SAMFI (Collaborative Group for Information Security) – This group, which is managed by MSB, also includes the National Defence Radio Centre (FRA), the National Post and Telecom Agency (PTS), the Swedish Armed Forces (FM), the National Police Board (RPS) and the Defence Materiel Administration (FMV).

SGSI (Swedish Government Secure Intranet) – Internet service that is not dependent on the internet, to which Swedish authorities can connect and which they can use to communicate with each other.

Social Engineering (social manipulation) – Use of various social stratagems to create confidence with the aim of getting someone to disclose

sensitive or confidential information. Phishing (internet fishing) is a form of social engineering.

SQL injections – Method that exploits security loopholes when handling input data in certain computer programs that use a database. The problem arises when input data coming into an SQL batch is not processed correctly by the programmer, whereupon an attacker can use special characters and commands in order to manipulate data or acquire information. The method is named after the database language SQL.

Trojan – Program that often contains malicious code and accompanies another file or program. It can then gain control and execute what it is programmed to do.

Part A Situational assessment

1 Introduction

1.1 Situational assessment

MSB's remit is to support and coordinate the work on societal information security and to analyse and assess outside developments in the area.[1] The situational-assessment work forms part of the monitoring of outside events and the analytical work, and constitutes support in the work on the national plan of action for information security administrated by MSB.[2]

The situational assessment constitutes support for players in society who are involved in managing information-security issues. The assessment is primarily based on developments during 2008 and the beginning of 2009.

1.2 What are information security and critical societal functions?

Information security means the ability to maintain the desired level of confidentiality, integrity and availability when handling information.[3] The term is broad, and concerns information in all its forms, including electronic information and hard copy. *Confidentiality* is the protective objective of preventing unauthorised persons accessing the information, *integrity* is information not being changed or destroyed without authorisation and *availability* is authorised access to the information in the desired manner and at the desired time. Information security is more than just safeguarding information systems; other resources, not least people's capabilities, are also important components of information security.

Fire, malicious code and hacking are just a few examples of *threats* that can cause loss of confidentiality, integrity or availability. *Vulnerabilities* in information management, e.g. the absence of fire protection and antivirus programs, mean an increased *risk* of threats causing disturbances and damage. What is crucial to the assessed magnitude of the risk is not only the consequences but also the likelihood of realisation of the threats. The risks can be reduced by various types of *security measure*, e.g. technical, legal, financial and organisational solutions.

[1] Section 6 Ordinance (2008:1002) with Instructions for the Swedish Civil Contingencies Agency (MSB)

[2] http://www.krisberedskapsmyndigheten.se/upload/17005/handlingsplan_samhallets_informationssakerhet_20080401.pdf

[3] SIS Handbook 550: Terminology for Information Security

Ultimately, work on information security is about standing up for a number of values and objectives in society, e.g. democracy, personal integrity, growth and economic and political stability.

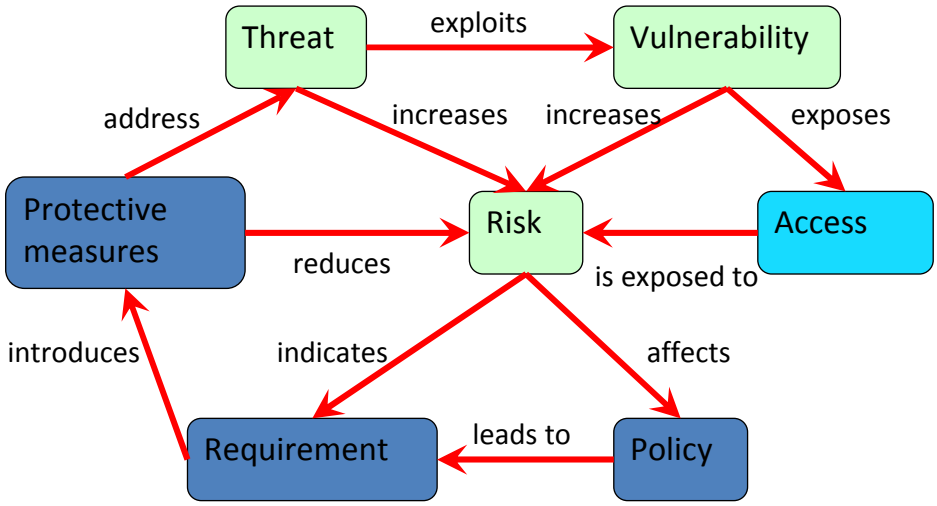


Illustration 1 Connection between parameters in the field of information security. SIS (Swedish Institute for Standards) Handbook 550: Terminology for Information Security

Efficient work on information security can be described in various ways. The model recommended in the regulations[4] of the Swedish Administrative Development Agency VERVA recommends clear responsibility, a well thought-out management system, and risk and vulnerability analyses with feedback.

The threats and vulnerabilities dealt with in the situational assessment concern information management that is of special importance from a societal perspective. This particularly includes information management in *critical societal functions*, as well as other types of information management where a lack of security has consequences for the functioning of society.

The following criteria are used here to identify critical infrastructure from an emergency management perspective:[5]

A shutdown or severe disruption in the function, singlehandedly or in combination with other similar events, can rapidly lead to a serious emergency in society.

The societal function is important or essential for responding to an existing serious emergency and minimising the damage.

[4] VERVA FS 2007:2 The Swedish Administrative Development Agency (VERVA) ceased to operate at the end of '08, but the regulations still apply.

[5] Swedish Emergency Management Agency, *Critical societal functions - Suggested definitions of essential functions from an emergency management perspective*

Efficient emergency management is to a large extent dependent on thorough preventive work. The standard of information security under normal conditions also largely determines how well society will cope with serious disturbances and crises when they occur.

1.3 Starting points

1.3.1 Introduction

Structured *situational assessment of societal information security* requires both a holistic approach and a selection method – the former in order to ensure that the data for the assessment is comprehensive and the latter to make sure that the areas dealt with in the report are those most relevant to the aim of the situational assessment.

1.3.2 Holistic approach

In this context a holistic approach to *information security* means that the assessment includes all information and information management and its need for confidentiality, integrity and availaibility. This means it is not sufficient merely to study technical solutions. User patterns, financial circumstances and legal regulation are also important. A number of parties play a major role in the design and level of information security. This involves everything from authorities, tele-operators, legislators, antagonists, standardisation organisations, technology developers and organisational management, as well as individuals. In addition to this, the requisite holistic approach includes everything from everyday security to security in crisis management.

The next stage is clarifying what we mean by societal information security. The concept is broad, and can mean various things. We have based the situational assessment on the government's description of societal security in the government bill 'Collaboration in the event of a crisis – for a more secure society'.

‘Societal security means events and circumstances that individuals cannot fully handle themselves and that threaten society's functionality and survival. At a fundamental level security means people feeling secure in their everyday life, and at a broader level it means the capacity to protect the values we associate with life in a modern democratic society. At the same time much of what is typical of modern society, including in the form of our advanced use of technology, is also what creates vulnerability.’ [6]

We have applied this approach to the field of information security. The plan of action for societal information security states that information security is a supporting activity to improve the quality of societal functions.[7]

[6] Government Bill 2005/06:133 p. 39

[7] Action plan for information security in Sweden 2008 p. 15

Deficiencies in information management lead to decreased confidence in services and the parties involved. Serious and repeated disturbances can lead to crises of confidence, which can spread to more parties and services, as well as to other parts of society. For example, decreased confidence in internet banks can infect other bodies that offer internet-based services.

Physical damage to critical infrastructure can also have fatal consequences. Incidents that lead to incapacitation or destruction of such infrastructure can lead to crises that affect financial systems, public health, national security or combinations of the same.

Dependence on functioning IT is constantly increasing throughout the world, as information management is increasingly being performed electronically. At the same time there is a clear growth in threats related to information security, e.g. hacking, fraud and dissemination of malicious code . The operators behind this include individuals, the organised criminal community and terrorists. In some contexts states have also been suspected.[8]

1.3.3 Information security and personal integrity

The issue of integrity is often raised in discussions of information security. Equally, information security is often touched on in discussions of integrity. We see information security as a tool to ensure that the selected level of protection of integrity can be maintained. Particularly in the management of electronic information, security is a necessity so as to be able to guarantee protection of personal integrity and of other fundamental freedoms and rights that will work in both an electronic and a physical environment. Most of the issues and areas dealt with in the situational assessment to a greater or lesser extent have a bearing on matters of integrity. To avoid any overlap, in Part B we have thus chosen to deal with integrity under the relevant heading, if necessary, and to leave general argumentation until the conclusions in Part A.

1.3.4 Selection method

With this holistic approach to societal information security as a starting point we have chosen to deal with areas and issues that are of particular interest in connection with *work on information security*, are particularly important to *society* and have changed, deteriorated or improved *during 2008 and early 2009*.

It should be emphasised that even though the situational assessment deals with information security from a Swedish societal perspective, an international outlook is necessary. Information technology creates a borderless society in which threats and vulnerabilities are no longer restricted to specific geographical conditions.

[8] Estonia, for example, asserted this after the attack in 2007, and the USA and Georgia also voiced this type of suspicion of other States.

1.3.5 Presentation and sources

Another aim of the presentation of the situational assessment is to reflect the holistic approach to information security and create an understanding for the conditions under which work on information security is carried out. Objectives, developments, threats and vulnerabilities govern which measures are and should be carried out. In the conclusions section we point to areas and issues that we deem are interlinked and need attention.

In order to create an overview the situational assessment starts with a summary. This is followed by two main sections. 'Part A Situational Assessment' deals with aims, starting points, objectives and conclusions. 'Part B Background' deals in more detail with developments, trends, threats, vulnerabilities and measures to increase the level of societal information security. The aim of this subdivision is to increase the accessibility of the material. A read-through of the 13 pages of Part A will provide basic understanding of information security and the issues that should be given special attention. If one or more areas are of particular interest to the reader, the chapter structure makes it easy to find further information in Part B.

The situational assessment is mainly based on information from open sources, a number of detailed studies, detailed interviews with parties in both the public and the private sector and a questionnaire-based survey aimed at government authorities. Confidential material has also been available for the work, but it is an open report, as sensitive information has been verifiable through open sources or has been raised to a general level. Most of the sources are recorded in the list of sources.

The work on identifying and prioritising important issues has been in collaboration with the Collaborative Group for Information Security (SAMFI), and the information-security committee of the Swedish Emergency Management Agency (KBM) and its working group for commercial issues.[9] Commerce and all authorities with a crucial role in the field of information security are represented in these committees and groups.

[9] KBM ceased to operate on 31 December 2008, and at the beginning of 2009 operations were transferred to MSB, together with the operations of the Swedish Rescue Services Agency and the National Board of Psychological Defence.

2 Objectives for work on information security

2.1 General objectives

The objectives for the work on information security at societal level are stated in the national strategy. The strategy is currently expressed in several versions with unclear status and mutual order. Work is thus currently in progress on updating and clarifying the strategy for societal information security.[10]

The first version of the strategy was expressed in the government bill 'Society's secure and preparedness', and included the following formulation of objectives.[11]

'The objective should be to maintain a high level of information security throughout society – sufficient to allow society to prevent or deal with disturbances to critical societal functions."

The government pointed out that the strategy to achieve this objective and other crisis management in society should be based on the principles of responsibility, equality and proximity. With regard to the distribution of responsibility between state and individuals, it was in principal stated that 'anyone responsible for information-management systems is also responsible for the system featuring the security required for the system to work satisfactorily.' The government bill also stipulates that the state bears overall responsibility for societal information security and must undertake the measures that cannot reasonably be the responsibility of individual organisations.[12]

Three years later the government supplemented the strategy with the bill 'Collaboration in the event of a crisis – for a more secure society', with the following wording:[13]

'The information-security strategy set by the government in 2002 should be developed to also include the capacity to detect, intervene against and take action in connection with disturbances in societally important IT systems. Confidence and security in using IT should increase. Increased security and improved protection of integrity should be striven for.'

[10] MSB was commissioned to submit proposals for an update of the national strategy on the basis of current societal developments. This work will also include formulation of objectives. The assignment will be reported on during 2009.

[11] Government Bill 2001/02:158 p. 103

[12] Government Bill 2001/02:158 p. 103

[13] Government Bill 2005/06:133 p. 89

The information-security investigation summarised its view of national strategy in ten points, which were in part based on the text of the government bills.[14]

1. To develop Sweden's position within the EU and in international contexts
2. To create confidence, security and safety, and to increase protection of integrity
3. To promote increased use of IT
4. To prevent and be able to deal with disturbances in information systems and communication systems
5. To reinforce the work of the intelligence and security services and to develop service of process
6. To reinforce capacity in the field of national security
7. To exploit society's combined capacity
8. To focus on critical societal functions
9. To increase awareness of security risks and possibilities of protection
10. To guarantee provision of staff

To sum up, it can be stated that alongside the objective of having a high level of societal information security and in particular being able to prevent or deal with disturbances in critical societal functions, few clear objectives have been formulated at a general level. The design of the various strategies indicates, however, that in addition to

- *Critical societal functions*

the following should also be seen as prioritised areas with regard to information security:

- *Confidence and protection of integrity*
- *Efficient utilisation of IT*
- *National security*

By and large all the strategic points mentioned can be allocated to the areas stated. This also applies to the sector-specific objectives dealt with below.

2.2 Sector-specific objectives

In a number of areas a decision has been taken to further clarify and specify the objectives for the work on information security and/or IT development in various strategy documents. This particularly applies to internet security, medical care and healthcare and e-government.

[14] Swedish Official Government Report SOU 2005:42 Secure Information, Proposals on Information Security Policy p. 111

2.2.1 Strategy for increased security for internet infrastructure

The objectives for the work on infrastructure and the internet are to be found in the strategy for increased security for internet infrastructure that the government adopted in 2006.[15] The government's vision is for the internet to be secure and fast and feature a high level of availability for everyone in Sweden within ten years. It is furthermore stated that it is important for individuals to feel confident that internet-based services and legal, financial and social interactions work securely and fast.

To achieve this, it is stated that security should be an obvious property of communication networks, programs and equipment, making the user's environment and communication secure. An important objective of the work of achieving this is to secure critical functions, i.e. functions which, if not maintained, create extensive disturbances or interruptions and thus impede or prevent use of the internet for large groups of individual users or for societally important companies, authorities and organisations. Large parts of the infrastructure are provided by private operators, and the public undertaking is based on requirements that the market itself cannot meet. [16]

2.2.2 National IT strategy for nursing and healthcare

In 2006 the government adopted a national IT strategy for nursing and healthcare, and emphasised IT as being one of the most important tools for renewing and developing nursing and healthcare activities.[17] It was stated that patient safety, quality of nursing and accessibility could be greatly improved through use of various forms of IT support.

In the strategy the need for information security is particularly linked to the work of creating a uniform information infrastructure. *'If it is in future to be possible to convey and interpret sensitive personal data electronically, both patients and healthcare providers must be able to rely on secure processing of the data. In order to guarantee the advantages of a national information structure and simultaneously tend to other important interests such as patient integrity and efficient healthcare, there is a need for an ordinance-regulated model for information security adapted to healthcare. We will thus get a defined minimum standard that promotes not only a secure exchange of individual data but also data quality and availability.'*[18]

[15] Strategy for Improved Security in the Internet Infrastructure N2006/5335/ITFoU

[16] Strategy for Improved Security in the Internet Infrastructure N2006/5335/ITFoU p. 5 f.

[17] National IT strategy for Nursing and Healthcare Government Communication 2005/06:139 http://www.regeringen.se/content/1/c6/06/03/73/9959f31e.pdf

[18] National IT strategy for Nursing and Healthcare Government Communication 2005/06:139 http://www.regeringen.se/content/1/c6/06/03/73/9959f31e.pdf p. 23

The strategy states that increased use of IT requires improved basic conditions in the form of uniform information structure, well-developed technical infrastructure for IT and changes in legislation.

2.2.3 Plan of Action for e-government

The plan of action for e-government[19] drawn up by the government in 2008 specify as an overall objective for public administration as a whole that by 2010 *'it must be as easy as possible for as many people as possible to exercise their rights, honour their obligations and take advantage of public administration's services. Where it is to the advantage of residents of Sweden and owners of companies and where quality, security and productivity can be improved, the authorities must collaborate by sector. Sweden will thereby resume a leading position in the area of electronic administration.'*

This objective must be implemented through work in four fields with different subtargets.

Regulatory framework for inter-authority cooperation and information management

- The authorities have regulatory frameworks that facilitate cooperation by sector in connection with e-government and efficient information management that makes the information easily available and useable, bearing in mind integrity and security aspects.

Technical prerequisites and IT standardisation

- The authorities have technical conditions that support the e-government work. An efficient, robust and future-proof infrastructure for electronic communication is to be promoted.
- The authorities have a security level that creates a high level of confidence in e-government. Standardisation of terminological and informational structures, interfaces for electronic services, electronic communication etc. are based on the joint needs of public administration or the sector and in agreement with international standards.

Joint operational support, provision of staff and joint follow-up

- Operational support that is common to the authorities is harmonised and automated to an appropriate degree with the aim of avoiding unnecessary costs and increasing joint productivity. The employees have the requisite skills to follow and drive developments. The state's joint IT costs are constantly followed up.

Public administration's contacts with residents of Sweden and company owners

[19]Plan of Action for e-government,
http://www.regeringen.se/content/1/c6/07/49/95/2c28b30b.pdf

- Residents of Sweden and company owners can easily implement and follow cases and have access to public administration's joint services and information.

All subtargets create requirements regarding work on information security within public administration.

3 Conclusions

3.1 Introduction

So that a situational assessment provides a picture of the level of societal security one must first present developments, threats, vulnerabilities, risks and measures carried out so as to then relate this to our objectives. Comparison of where we stand on where we want to get to gives us a basis for prioritisation of the areas to which we need to devote particular attention.

In Chapter 2 we listed the objectives at general and sector-specific levels. It can be said that their design is relatively general throughout, and that they can only be deemed measurable to a limited extent.[20] But they provide a pointer regarding the areas that are deemed particularly important from a societal standpoint. In the situational assessment's conclusions we have thus chosen to particularly study:

- Critical societal functions
- Confidence and protection of integrity
- Efficient utilisation of IT
- National security

3.2 Critical societal functions

Digital control systems (SCADA) that control the electricity and water supply and other basic infrastructure are core components of critical societal functions. The area has attracted increased attention as a result of the creation of a public, available and easy-to-use attack code that exploits a well-known vulnerability in a relatively well disseminated SCADA system. Vulnerabilities arising when older SCADA systems are connected to modern administrative systems still persist, and bearing in mind the increasingly sophisticated threats their management has become a priority. It is important that more measures in this area be carried out over the coming years.

IT-related threats are directed at critical societal functions such as financial services, media companies and medical care and healthcare.

[20] As an example of a relatively measurable objective: Residents of Sweden and company owners can easily implement and follow cases and have access to public administration's joint services and information.

- During the course of the year medical care and healthcare have been affected by several incidents that have resulted in patient records becoming unavailable and medical equipment being affected. Both technical and administrative deficiencies in electronic information management have been demonstrated which, when seen together with threats such as malicious code , create a major need for increased information-security measures.
- Information indicates that media companies have in certain instances neglected to report hacking for fear of reprisals. This could lead to serious consequences from a societal standpoint, as criminals can influence media reporting and increase the number of unrecorded cases.
- In the financial sector it is chiefly the customers who are vulnerable, and the attacks are targeting weaknesses in their security systems or shortcomings in their awareness of security.

Cybercrime is a complex threat to critical societal functions. Crime-fighting is in part impeded by a lack of resources, undisclosed cases and problems that are hard to categorise. Businesses are handling events internally as technical problems, whilst they are by the same token being exposed to cybercrime. Security work and crime-fighting related to IT constitute a field in which private companies are occupying an unusually large area and are assuming particular responsibility. A problem of this role distribution is that the boundaries between crime and incident are blurring and crime-fighting authorities are losing their overview of cybercrime. Unlike crime-fighting authorities, those committing cybercrime are not bound by legal and geographical boundaries. The creation of functional and efficient international regulatory frameworks and conventions calls for harmonisation of national regulatory frameworks. We thus see a big need for increased international collaboration on both legislation and crime-fighting. An important step is the EU Commission's 2007 general-policy initiative to improve European and international coordination of the fight against cybercrime.

The internet constitutes a fundamental part of societal electronic infrastructure. Robustness is a prerequisite for availability of and confidence in the services provided electronically. In this context we wish to draw attention to the fact that use of the DNSSEC security protocol is still limited, despite a gradual increase. With regard to time, both the dependence on disturbance-sensitive time sources and the lack of signed time sources in the form of signed NTP servers (Network Time Protocol) should be taken into account by those operating critical infrastructure. Signing central Swedish NTP servers is a relatively simple measure, which alongside PTS's work on reducing societal dependence on disturbance-sensitive time sources may contribute to increased confidence in internet functions. The work on reducing the number of unprotected wireless networks is more complex, and should be carried out through measures for users and retailers. Access to secure products is also an important part of an infrastructure, and we deem the work on the Common Criteria standard to be important.

3.3 Confidence and protection of integrity

Appropriate protection of personal integrity and other fundamental freedoms and rights are prerequisites for the creation of well-founded confidence in various e-services in society. Developments in the field of IT are fast, and personal information is being handled in an ever more sophisticated way. In a number of social sectors extensive investments in increased use of electronic information management are taking place – not least with regard to e-government and medical care and healthcare. New technology and changed user behaviours/new services have also facilitated access to personal information. In the field of technology attention should be drawn to RFID, and development of Web 2.0 through user-friendliness and user-controlled content has not infrequently led to increased access to personal information, e.g. through social networks. Dissemination of malicious code through social networks is a growing threat that may have a direct effect on confidence in services.

Legislation has also changed access to personal data, as for crime-fighting reasons the legislator has given copyright holders access to information that was not formerly accessible. Regarding crime-prevention activities, the Act on Signals Intelligence in Defence Operations should also be mentioned, as in the quest for technical neutrality conditions have been created regarding signals surveillance both over the Ethernet and via cable. Regulation has also contributed towards clarifying protection of integrity in certain areas, e.g. the Patient Data Act and once again the Act on Signals Intelligence in Defence Operations.

Efficient crime-fighting can to a certain extent hamper protection of integrity whilst simultaneously promoting it. To create confidence in information management in an electronic environment it is important for fighting of cybercrime to be perceived as being efficient. At the same time the balance between protection of integrity and crime-fighting must be appropriate.

There is an awareness of the importance of protection of personal integrity, which is reflected in several of the measures for increased security that were carried out in 2008. For example, all the recorded plans of action contain a number of measures that promote integrity. In accordance with the government's plan of action for e-government, electronic identification is an important factor for confidence and dialogue between authorities, residents of Sweden and companies. In many cases there is a need for secure identification, a requirement for a signature and protection of personal integrity.

The objectives related to confidence and personal integrity express a striving for increased utilisation and creation of efficient e-services, whilst the need for protection of personal integrity is simultaneously emphasised. Deficiencies in crime-fighting, vulnerabilities in e-government, a high frequency of identity theft and theft of card information indicate that we have not yet achieved our objectives. In order to achieve and maintain adequate protection, we think there is a need for a holistic approach to protection of personal integrity, which can be attained by combining technology, the law and user patterns. It is of particular importance to monitor technological developments and make sure

that regulation provides clear support and unambiguous parameters for protection. In this discussion it is important to underline that the scope of protection of integrity must sometimes be restricted because of crime-fighting. As an initial stage we think it is very important to implement the measures advocated by the plans of action, whilst at the same time legal regulation of protection of integrity should regularly be reviewed so as to ensure that its design is adequate and appropriate in relation to its objective.

3.4 Efficient use of IT

Efficient use of IT presupposes both administrative and technical security. This brings a number of different areas to the fore, and we wish to direct particular attention to outsourcing (external handling of services), new user patterns and continuity planning.

External service providers are handling more and more societal information and the concomitant safety issues. The level of customers' requirements varies greatly, and this can be the result not only of lack of knowledge about security requirements and ingenuousness regarding threats but also cost restraint. The public sector is largely governed by the Public Procurement Act, and many authorities use price as the sole criterion when evaluating incoming offers. In many instances both public and private customers place too much faith in the security that forms part of the basic service, and formulate their agreements accordingly. We think the lack of awareness of the problems is serious, and deem there to be a need for competence-raising measures and possible regulatory review.

New user patterns in conjunction with increased mobility and access to Web 2.0 services bring new risks for organisations. This should lead to more extensive security work, but the will to use fast technological development and the striving for user-friendliness often mean that security considerations come second.

Continuity planning is a fundamental part of the internal security work on safeguarding an organisation's business. Deficiencies have been identified in several contexts; for example, investigations during 2008 showed that municipalities are displaying deficiencies in their work on counteracting and documenting stoppages in their operations and protecting critical procedures from the effects of unforeseen serious stoppages or catastrophes. This indicates a need for measures to promote systematic work on information security.

Users have to be able to rely on internet content and protection of sensitive information on websites. During 2008 a large number of attacks on databases or database servers linked to websites were recorded. The underlying problem with website security is often a lack of processes and control, and absence of security tests, analyses etc. Many websites are not designed for a large number of users from the start, and user-friendliness and functionality have been emphasised rather than well-functioning work on information security. The number of people setting up and administrating websites is also often small in relation to the number of users. Attackers exploit this and use various methods of attack to achieve their aims.

An increasingly complex IT environment and an increasing number of integrated networks mean that the focus is often on more restricted and manageable IT-related problems in one's own organisation. It is also important to draw attention to and analyse consequences and connections from a societal perspective. To facilitate exploitation of the potential of information technology and create the requisite confidence, build-up of basic information security and expertise in the field of information security are crucial. Both items are proposed measures in the plan of action for societal information security.

3.5 National security

The events in Georgia and latterly Israel/Gaza indicate a development towards conflicts in which traditional armed combat takes place in parallel with information operations. The potentially asymmetrical nature of information operations makes it hard for the nation affected to know what response is appropriate, as there may be great uncertainty about who the attacker is. It is feared that there will gradually be operators with sufficient information and the skill and desire to carry out cyberattacks that may destroy critical societal functions and put it out of action.

The threat to states currently posed by information operations calls for a new view of security. We have hitherto seen examples of cyberattacks that are intended to destabilise a country, disrupt informational channels in conjunction with armed combat, affect decision-makers and recruit sympathisers. We assess that parallel use of information operations and armed combat in conjunction with conflicts will continue and will develop. From a Swedish perspective the most likely scenario still appears to be effects on societally important infrastructures in the event of any future attack, but it is also important to be aware of the risk of manipulation of information.

We assess that a continued focus on international collaboration is necessary in order to be able to counter the form of asymmetrical threat posed by information operations and so as to be better equipped for large-scale network attacks of the type that has recently affected several nations.

3.6 Comparison with the situational assessment for 2008

The situational assessment for 2008 focused on threats and vulnerabilities/risks. This section is a brief summary of a number of the conclusions presented in last year's situational assessment. So as to create an overview they have been structured in accordance with the same main objectives used in the handling of objectives in the situational assessment for 2009.

Critical societal functions: Attention was drawn to the threat of attacks on digital control systems. It was stated in this context that many countries equipped themselves so as to be able to resist feared attacks on critical infrastructure such as electricity supply, water purification etc. American reports indicated successful attacks on electricity networks.

Confidence and personal integrity: The problem of sensitive personal data being passed on to unauthorised persons was particularly emphasised. Examples are illegal trade in bank accounts, log-in details, ID numbers and credit-card details. There have been instances of blackmail based on the threat of disseminating sensitive information on individuals and companies. Internet fraud was the commonest cybercrime against individual Swedes, and there were phishing campaigns against bank customers in both 2006 and 2007. Legitimate websites were manipulated to facilitate access to individuals' computers and information.

Efficient use of IT: The report stated that dependence on IT is on the increase, especially in businesses such as healthcare and the financial sector – which at the same time means increased vulnerability. Examples are introduction of e-services and outsourcing. The majority of IT-related incidents in Swedish authorities are still caused by administrative deficiencies, including absence of policies and continuity plans. Over half of authorities experienced incidents in 2007. Operational disruption occurred in IP telephony, the government's website and Teracom's operations.

National security: Large-scale information operations of the type that affected Estonia are an established risk. The USA, Great Britain and Germany suffered an increasing number of attacks on authorities in 2007. The prediction is that the scope of cyber-warfare and government IT-based intelligence operations will grow, but the threat of terror against Sweden was not deemed to be particularly high in 2008. Criminal groups created extensive networks, with the various roles divided up among different countries. Two trends were emphasised:

- An increasing number of small, targeted attacks,
- Large networks of hijacked computers that can be rented commercially for use in attacks

Incident reports were characterised by a large number of unrecorded cases, regarding both organisations and individuals.

Part B Background

4 Information management, development, and trends in 2008

4.1 Introduction

Technical developments and changed user patterns are affecting the work on information security. A true analysis of needs and deficiencies with regard to security measures must thus be rooted in the actual environment in which the work on information security is to be carried out. In the present chapter we have chosen to select a number of development trends that we deem to be of great importance to the design of the work on information security. Even though technological development is a prerequisite for several of the trends, it is often only changed user behaviour patterns that give rise to more extensive security considerations. All sections contain a brief description, a record of the trend's importance from both information-security and societal perspectives, assessment of developments during 2008 and discussion of the consequences and opportunities of these developments. We assess that the development of cloud computing is of particular interest, as it is predicted that use of the service concept will greatly increase. An understanding of the service's structure is of great importance to secure and appropriate handling of threats and vulnerabilities. Web 2.0 services are also of interest from a security standpoint, as they both change users' communication patterns and make the boundaries between private and professional life harder to differentiate. Both of these facilities may have a crucial effect on choice of information-security solutions.

4.2 Increased mobility

In the longer term we are seeing development towards increased integration with the mobile world. Despite security incidents, security is not yet a major user requirement, thus handling of problems is not infrequently being postponed. There is instead more of a focus on increased functionality and user-friendliness. Vulnerabilities are dealt with in greater detail in Section 6.3.1 Mobile Units.

4.3 Web 2.0

Developments on the internet are towards a more user-controlled environment with a high level of interactivity. This way of using the internet is called Web 2.0 and includes Facebook, bilddagboken.se, Wikipedia and blogging. What differentiates this type of application from more traditional ones is the fact that users themselves control information far more than before. Developments are to a large extent governed by user benefit and not primarily new technical solutions. These applications are currently being used both privately and within commerce and public operations. The boundary between work and private life

is being erased, and the vulnerabilities of technical solutions can thus be exploited to gain access to organisations' internal networks. With regard to technical security, there are deficiencies in both social networks and blogs.

The big increase in instant-messaging services (AOL, Yahoo, MSN Messenger etc.) has brought fresh problems for companies that older security solutions cannot cope with. As it is easy to transfer files by means of instant messaging, the method has in many contexts become increasingly prevalent.

4.4 External handling of services (Outsourcing)

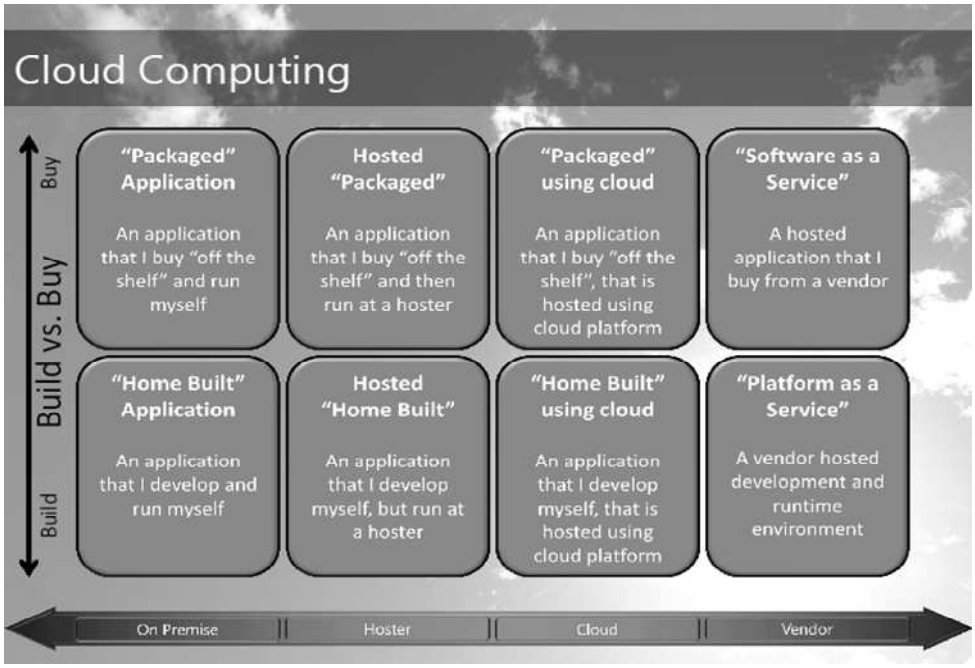
There is a development towards external service providers handling more and more of society's information and the concomitant safety issues. There are many *advantages*, e.g. cost savings, the often greater robustness of operation and administration, and access to the suppliers' often high technical capacity and level of expertise. The *disadvantages* include the creation of a dependency relationship between purchaser and supplier and the weakening of the purchaser's level of expertise (above all in the longer term). The dependency relationship means it may be hard to withdraw business once it has been placed with a service provider.

Companies such as Microsoft, Yahoo and Google are now building large computer centres in the USA so as to be able to offer a number of different services. Their customers no longer need to store data, programs or applications on their own servers, as this service is provided by the supplier. Information management and program control takes place over the internet. This set-up is often called Cloud Computing[21], and has attracted great attention over the past year. Currently, however, the service is only at the developmental stage, and has not been implemented on a large scale. In some quarters people are dubious about Cloud Computing, chiefly with regard to security. In future, however, companies may have no choice in the matter, since IT infrastructure has grown enormously and companies' computer centres are now often made up of a complex of underused hardware the operation of which is requiring more and more staff, space and electricity. Financial developments also mean that companies are constantly having to become more efficient, and are thus choosing outsourcing. One of the advantages is that companies can reduce their IT investments and IT staffing, meaning they have money left over for product development and can concentrate on their core business. The increased need for storage capacity makes the purchase of storage as a service instead of buying and administrating more and more disks and servers a positive feature for many people. It is currently above all the smaller companies that are the

[21] For further information
http://www.economist.com/specialreports/displayStory.cfm?STORY_ID=12411882

most positive about this, as they themselves often lack these services providers' expertise and experience in running big computer centres.

There are several different types of Cloud Computing. The illustration below represents an attempt to clarify the different options currently available to companies and management.



Source: Microsoft

Deciding between the advantages an option offers and the possible security consequences is an important balancing act. There are several security considerations when a company or administration is today planning to outsource parts of their systems or business to an external supplier. Part of their control will be lost, and in many cases the information will be managed in another country with different laws and regulations – which may have consequences. The organisation has to decide whether it is only permissible for their data to be managed within Sweden, or whether this can be done within or even outside the EU.[22] Other security-related questions that should be asked are: How does the supplier carry out backup? How is data safeguarded against hacking and other improper use? Can you rely on nobody else accessing the information and on its being available without delay and interruption? Can you rely on the company providing the service still being there in a year's time? Is it easy to switch service providers? What is legal regulation like?

[22] Not only are the regulations of the Personal Data Act (1998:204) updated, but other regulations may also be applicable, e.g. the Security Protection Act (1996:627).

4.5 Virtualisation and Service-Oriented Architecture

More and more organisations are using virtualisation, and it looks as if this tendency will be continuing. If vulnerabilities arise in the products used to create virtual servers, it is possible to access not just one but all of a company's servers. There can be a high level of damage if you run all virtual servers on the same machine. In this context the same approach to security is required as with other information management.

As a consequence of the rapid changes taking place in business today and the fact that many systems do not function together, various forms of IT support have been developed so as to facilitate provision of greater flexibility. Service Oriented Architecture (SOA) is a well-defined concept in this field, the aim being for standardised interfaces to facilitate mutual communication between different systems and applications. Many analyses, however, show that during 2008 there was a decline in interest in SOA, or rather the concept per se. The benefit of standardised interfaces for electronic services remains, but they are being developed in new forms and under other names.

4.6 Data Loss Prevention

Data Loss Prevention (DLP) allows organisations to prevent sensitive information leaving an organisation and falling into the wrong hands. There used to be a focus on preventing intruders, but as loss of information has become a bigger problem the need for this type of technology has increased. It is often hard to not only prevent loss of information but also detect such a loss. DLP can be created in several ways, e.g. by creating obstacles to copying of sensitive information to USB, stopping the Copy & Paste function, ensuring that access rights are adhered to/not changed, and protecting against transmission of information by email or instant messaging.

DLP is still a relatively new concept and has not been made into any overall solutions, but constant development is in progress and functions are being incorporated into various types of security products. Implementation of a DLP solution requires detailed analysis of an organisation's data so as to identify information worth protecting and give it a security classification. One reason why organisations are holding back on full implementation of DLP is that it is considered to be extensive and expensive work.

4.7 Radio Frequency Identification

Radio Frequency Identification (RFID) is a technology for reading and saving information in an RFID chip, which can basically be said to comprise a radio receiver, a memory and a radio transmitter. The RFID chip is usually described as being a replacement for today's barcode, but it differs from the latter in that an RFID chip is unique. The technology is being used in more and more areas, e.g. Swedish passport documents, stock goods, medical packaging, entry systems and public transport. The chip makes it possible to collect information on a specific product and trace its geographical location without any physical contact. The technology is relatively cheap, and there are many applications.

Serious security deficiencies were detected during 2008, and they are recorded in greater detail in Section 6.3.3.

4.8 Altered behavioural patterns as a result of new legislation

Several regulatory frameworks which in our assessment may cause users to change their handling patterns came into force or were prepared during 2008 – in particular the `Act on Signals Intelligence in Defence Operations (2008:717) and the changes in the regulatory framework regarding intellectual property rights[23], based on the so-called IPRED Directive. Both give selected groups increased access to certain information that was not previously available.

According to the Act on Signals Intelligence in Defence Operations, FRA can under certain circumstances carry out signal surveillance using cable for traffic crossing national borders. This contrasts with the previous situation, whereby this type of surveillance was only permissible over the Ethernet. The reason for this easing-up was a striving for technical neutrality. The Act regulates both integrity considerations and approach. See further in Section 7.3.2.

The changes in copyright law make legal proceedings regarding breach of copyright easier by giving copyright holders the right after a court decision to request information from tele-operators on who holds the IP address to which copyright-protected material has illegally been downloaded.[24] The regulatory change is based on an EC directive[25], and its aim is to counteract breach of intellectual property rights. See further in Section 7.3.2.

The debate on the regulatory changes has concerned integrity issues and has at times been intense. This type of issue has also attracted attention internationally, e.g. the integrity discussions a few years ago regarding the Echelon signal-surveillance system.[26] Both the regulatory changes and the related debates may lead to increased use of encryption as a way of impeding access to the content of traffic. A reduction in the number of unprotected and non-encrypted wireless networks is another possible development,[27] the aim

[23] Government Bill 2008/09:67 proposes an amendment to the Act on Copyright in Literary and Artistic Works (1960:729), the Trade Marks Act (1960:644), the Patents Act (1967:837) etc.

[24] There will otherwise be no changes regarding the requirement for evidence. It is still necessary to show who was sitting at the keyboard in connection with illegal download of copyright-protected material.

[25] Directive of the European Parliament and the Council 2004/48/EC of 29 April 2004 on the Enforcement of Intellectual Property Rights

[26] See for example http://www.europarl.Europe.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN and http://www.cyber-rights.org/interception/echelon/

[27] In 2008 KBM carried out an investigation of the number of unencrypted wireless networks in three major towns, and there may be reasons to repeat the investigation over the coming years so as to detect any changes.

being to prevent unauthorised persons using an unprotected wireless network to download copyright-protected material.

5 Antagonistic threats

5.1 Introduction

An antagonistic threat presupposes an operator (antagonist) who intends and is able to perpetrate harmful actions. Non-antagonistic threats usually include natural catastrophes and technical faults whereby the common denominator is a lack of intention and of a clear sender. We have chosen to jointly address the frequently occurring difficulty of differentiating between non-antagonistic threats and vulnerabilities in Chapter 6.

The antagonistic threats we list in this chapter have been divided up according to aim: threats that target society as a whole and threats that target individuals/organisations. There is no clear dividing line between the two areas. Extensive attacks on a large number of organisations not infrequently have consequences at societal level, and direct attacks on critical societal functions, e.g. infrastructure, in practice often mean attacks on specific individual organisations. Despite the problem of drawing a dividing line we have chosen to subdivide, chiefly so as to clarify the range with regard to the aim, scope and consequences of the antagonistic threats.[28] All subsections include a brief description, an account of the significance of the threat from an information-security standpoint and from a societal perspective, assessment of developments during 2008 and discussion of the consequences of the threat. Of particular interest to us is the development of threats to *digital control systems* (SCADA), which previously only concerned administrative systems. The area of information operations is also interesting, as we see in it a trend towards situations in which armed conflict will continue to take place in parallel with cyberattacks.

5.2 Societal level

5.2.1 Threats to critical societal functions

By following the development of the threats in our critical infrastructures, we have observed certain trends. We have chosen to highlight the following example, which we consider to be of particular interest, bearing in mind the initially described objectives of being able to prevent or deal with disruption of critical infrastructure, consideration of confidence and protection of integrity, and efficient use of IT. Under the heading *Information operations*

[28] As a basis for the chapter's observations and assessment we have used the results of a collaborative project involving the Council for Crime Prevention (BRÅ) and KBM, who were also the assigners, regarding strategic IT incidents that may have consequences for critical infrastructure.
BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008

circumstances are described that more directly link to questions of national security.

- *During 2008 the area of digital control systems (SCADA systems) attracted increased attention in that for the first time hitherto it involved the creation of publicly accessible, easy-to-use attack code that exploits a well-known vulnerability in a relatively well disseminated SCADA system.*

To sum up, it is very hard to give a clear picture of the antagonistic threats to SCADA systems in critical infrastructure. SCADA systems constitute a critical part of the systems that supply society with electricity, heating, drinking water, fuel and transportation. Unlike administrative systems, where a delay can be acceptable and availability deviations can be tolerated, SCADA systems control time-critical activities, thus the availability requirements are very stringent. These systems used to be well protected by virtue of their isolation from other systems and safeguarding by means of good physical security.[29] As a result of integration with office networks, SCADA systems are now to a large extent exposed to the type of threat that previously only affected administrative computer systems. During 2008 the area of digital control systems (SCADA systems) attracted increased attention in that it for the first time hitherto involved the creation of publicly accessible, easy-to-use attack code that exploits a well-known vulnerability in a relatively well disseminated SCADA system.[30] SCADA security has for many years been dealt with at hacker conferences, and relatively detailed technical discussions are in progress in various forums. Recently the field also seems to have attracted increased attention amongst less well-qualified hackers, and second-hand equipment used in control systems is now sought after – and offered – in various contexts on the internet.

- *Instances of hacking into authorities have been established whereby confidential information became accessible to the organised criminal community.*

Even though we are only talking about a few cases, from a societal standpoint it is very serious if criminals can access confidential information from our authorities. Information on the authorities' work and approach has previously proven to be highly sought after in criminal circles. If people perceive that their personal data is not being stored securely this will constitute a threat to personal integrity, and will become a societal problem if residents of Sweden lose their confidence in the authorities' expertise and ability. DDoS attacks and overload attacks are otherwise everyday occurrences for most authorities, and

[29] E.g. locked doors, alarms and fences

[30] Read further Chap. 6.2.2

in most instances they do not have any serious consequences, but are handled using technical protection.[31]

- *Fraud in the financial sector is chiefly aimed at users.*

The Swedish banks generally have a high level of security, so fraudsters exploit deficiencies in individuals' security systems or their security awareness.[32] Financial services are one of the main fields that are of strategic importance to the functioning of Swedish society. In this area damaged confidence is one of the major threats, as internet-based financial services are currently used extensively. Undermining of confidence in internet-based financial services could be of great significance to society. Continued development of threats to users may lead to banks being asked what security requirements they can impose on users. When banks' systems are not under attack they are under no legal obligation to compensate defrauded customers, but they often choose to compensate those affected by internet fraud, provided they have reported the crime to the police.[33]

- *Data is available on media avoidance of reporting on hacking and information theft.*

Media companies have refrained from reporting on data incursion that has affected them or competing media companies. In at least one case a company that has been subjected to hacking and publication of its sensitive information on the internet has stated that it did not dare to proceed with reporting the matter to the police because it was afraid of escalation of the attacks. They also suspect that competing media companies are refraining from reporting on the event so as to avoid becoming a target for these groups themselves.[34] In a democratic system the media has the remit of screening society and providing information on important events. The suspected widespread fear of reprisals from attackers if a matter is reported is thus particularly alarming, as the media's credibility as an objective reviewer and conveyor of news could be undermined. Like other organisations, media companies are frequently subjected to attempted DDoS attacks, overload attacks and hacking. The majority of these are dealt with by means of technical protection.[35]

---

[31] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 33

[32] What are common are so-called man-in-the-middle attacks, whereby the fraudster first infects the victim's computer with a trojan. When the customer then tries to log into his bank account on the internet the fraudster shows a false website, where the customer enters his log-in details. The fraudster can then use the log-in details to transfer money from the victim's account.

[33] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 22

[34] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 36

[35] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 34

5.2.2 Information operations

Information operations (IOs) can be used as a form of non-military exercising of power, and as a complement to conventional military measures. Information operations can constitute an asymmetrical[36] threat, which means that attacks on a nation can be carried out by anything from another state to a small group of individuals or even by a single individual. The tools used are often the same as in everyday peacetime acts. The attacker is also at a great advantage in that attacks can be carried out anonymously.

The concept of IO is chiefly used in the USA and within NATO. In Sweden there is not yet any official definition, but the Swedish Standards Institution SIS defines the concept as follows: *'Joint and coordinated measures in peacetime and at times of crisis and war in order to support one's own political or military objectives by affecting or utilising an opponent's or another foreign operator's information and/or information system whilst simultaneously using and protecting one's own information and/or information system. The ultimate objective is to affect human decision-making. Information operations can be both offensive and defensive.'*[37]

Information operations can be carried out as cyberattacks, e.g. by illegally hacking into a computer system, or they can involve the capacity to use various networks for communication or an act with the aim of manipulating information. There are various techniques of achieving any of these aims, e.g. planting malicious code in various systems so as to covertly steal important information. Information operations can also be carried out using overload attacks on a system with the aim of destroying an activity or completely putting it out of action.

The following are examples taken from news items over the past year.

Data espionage
The Finnish State and companies in the Finnish weapons industry have been subjected to data espionage. One or more employees have received email containing viruses, thus allowing the attacker to access information on individual handling agents' computers as well as password-protected networks. The first attacks took place in 2004, and attacks have subsequently become more frequent. The increase during 2008 was dramatic. Some of the attacks have been traced to China, but this does not mean they were carried out from there. The nature of the attacks was that employees received emails from a colleague or other known person concerning meetings or other physical events. These emails contained Word, Excel or PDF attachments containing malicious code adapted for the attack. Their computers continued to work completely normally following infection.[38]

[36] Asymmetrical threats are threats based on the fact that a technically or materially weaker party can also adapt and utilise his behaviour to exploit the opposite party's weaker sides in terms of resources, politics or psychology. From Swedish Official Government Report SOU 2004:32, p. 19

[37] Swedish Standards Institute (SIS) Terminology for Information Security Edition 3, 2007

[38] 'Delete' Newsletter No. 78,

DDoS attacks/overload
Several websites that are run by Radio Free Europe and that target Belarus were for two days overloaded in an attack involving around 50,000 ping calls a second. The attack started on the anniversary of the Chernobyl Nuclear Power Station disaster, and Radio Free Europe covered demonstrations in which thousands protested against the fact that many people affected had not received any compensation and against the government's decision to build a new nuclear power station. Radio Free Europe is financed by the USA, and its remit is to disseminate information in countries where democracy is threatened.[39]

A further example of an information operation is when defects at the production stage are deliberately inserted into hardware and software, which is then sold to authorities and/or companies. Seldom is any individual producer or country singled out in such instances. Information in the media refers to the US Air Force's December 2007 analysis, which demonstrated that much of the Pentagon's operating systems comprises so-called COTS components (standard products) manufactured abroad. Cost is cited as the reason for buying these products and creating exposure to risks.[40]

5.2.3 The militarisation of the internet

The internet was originally created as a military project, but in the course of time it has become essential to all forms of operation, though without being covered by any common international regulations. The internet can now be used to create threats to national security, and many countries' military forces are preparing for both defensive and offensive handling of cyber-threats in future conflicts.[41]

IT-related attacks or cyberattacks are characterised by the fact that the tools used are the normal tools utilised in the constant small-scale attacks. It is thus unlikely that an attack tool on its own could cause great damage – it is rather a combination of several methods and tools and a high capacity that could lead to a dangerous situation. Acquisition of the relevant intelligence about preparations for an attack has thus proven to be very important, and is vital to presentation of an overall situational depiction.[42]

Cyberattacks have lent a further dimension to modern-day conflicts. More and more countries state that they are being subjected to cyberattacks linked to particular security-policy situations. The large-scale internet attacks on Estonia

www.hs.fi/english/article/Finnish+state+and+armaments+industry+appropriate+by+online+espionage/1135237080345

[39] 'Delete' Newsletter No. 76, http://www.securityfocus.com/news/11515
http://sakerhet.idg.se/2.1070/1.159392

[40] Council on Foreign Relations, *The Evolution of Cyber Warfare*, Greg Bruno, Staff Writer February 27, 2008, http://www.cfr.org/publication/15577/#2

[41] http://www.ccdcoe.org/8.html

[42] The ability to quickly put together a staff function involving players from all relevant fields proved very valuable in the Estonian handling of the attacks in 2007.

in May 2007, when the media's and the authorities' internet services were put out of action by overload attacks, are the ones that have attracted the greatest media attention. The world was reminded of the information society's vulnerability, provoking questions about information operations as a non-military tool for exercising of power.[43] The events were afterwards described in the media as constituting one of the biggest and most sophisticated cyberattacks ever on a sovereign state.[44] Some experts, however, assert that what we saw was merely the tip of the iceberg, bearing in mind the number of attacks taking place. Several states have repeatedly been singled out in the media for having carried out similar attacks. All accusations are usually rejected by the countries in question.[45]

The events in Estonia[46] were followed by a number of incidents during 2008. In August 2008 Georgia was hit by coordinated cyberattacks against the Ministry of Foreign Affairs' website. The attacks are said to have borne many similarities with the events in Estonia in 2007. One big difference was the fact that the cyberattacks in Georgia took place in parallel with armed combat on the ground. A serious consequence of such attacks is an adverse effect on society's ability to function and rule, as a result of damage to a country's capacity to communicate with its citizens and keep them informed. Georgia, whose IT development has not progressed as far as that of Estonia, was probably affected more by the armed combat than by the digital attacks.

In conjunction with the Israeli attacks on Gaza in January 2009, it was stated that both Israeli and Palestinian websites suffered attacks in the form of *defacement*[47]. This practice is usually called *hacktivism*, i.e. a combination of hacking and political activism, and it has been observed in a number of previous conflicts.[48] Both sides stated that they had distributed tools to carry out certain attacks on the opponent's websites. Recruitment of sympathisers through the internet is a method that has been used on several occasions.

Opinions differ as to whether there is a threat in the form of cyberwar, and if so, what it is. There is as yet no definition of when a cyberattack is equivalent to an armed assault, nor any common strategy regarding the countermeasures that could then be considered legitimate.[49] One method that seems to be gaining popularity amongst international operators can in essence be described

[43] http://www.aff.a.se/vf2008_2/Information%20Nicander%20sid%2036.htm

[44] Computer Sweden 12.06.2007

[45] Council on Foreign Relations, 2008

[46] The large-scale network attacks on Estonia have led to a number of initiatives within NATO that are described in greater detail in 7.5.5 *International Cooperation*

[47] Defacement often involves an attacker replacing an original website with a new one, not infrequently containing a political message. The activity has sometimes been described as electronic graffiti.

[48] http://www.theregister.co.uk/2009/01/09/gaza_conflict_patriot_cyberwars/

[49] See further under 6.2.8.3 for an international-law perspective.

as a number of set criteria that must be met for an attack to be deemed equivalent to an armed attack, namely:

- The event must have caused major damage
- National borders must have been forcibly crossed
- What occurred must have taken place within minutes or hours
- The attack must have been directed at a specific target.[50]

One of the challenges we face is measuring the risk of attack. Some experts maintain that continuous attacks are taking place as part of what might be called a 'silent' cyberwar in which soft targets are attacked further out in the chain in the form of products, with the aim of then making an assault on the primary objective. The reason for attacking these components is given as being the fact that security is less robust there. And ongoing occurrences such as this are said to be less dramatic than a traditional terrorist attack, thus escaping detection.

The targets and consequences of cybercrime can be of the same nature as politically or militarily motivated acts. One example is an event in February 2009, when, according to statements, take off of French attack aircraft, was prevented by a data virus that had infected an internal computer network, where the necessary instructions were to be found. The underlying reason was probably that previously issued warnings about this computer virus from the IT company affected had been ignored by those concerned.[51]

It is feared that in the course of time there will be operators with sufficient information and the requisite audacity to carry out cyberattacks big enough to disrupt important national infrastructure and put it out of action.[52] Several commentators think that cyberattacks in the form of actual internet attacks will become a normal component of future conflict situations, in parallel with armed combat.[53]

When a country suffers an attack it is not inconceivable that assistance will be contributed by a third party, e.g. by technical experts or, as in the case of Georgia in 2008, through the transfer and establishment of several authorities' websites in other countries as a way of escaping the attacks. And NATO, who recently developed a cyber-defence policy and a concept for cybersecurity issues, also sent people to Georgia by way of support in face of the attacks. What happens if a third party is seen as a party in an ongoing conflict?

[50] So-called 'Smith's Analysis', information from *Cyber Warfare conference*, Defence IQ PC, London 2009
[51] French fighter planes grounded by computer virus, Daily Telegraph, 07 Feb 2009
[52] McAfee, *Cybercrime cyberlaw Constant Threat of National Attack, 2008*
[53] Among others:http://www.ccdcoe.org/8.html

5.3 Organisational and the individual level

5.3.1 IT-related crime

IT-related crime or cybercrime[54] can be 'an act that involves prohibited access to or influence on an information system'[55], and a further advance involves criminal acts whereby the computer is used as a tool or aid in crime, e.g. when the internet has facilitated establishment of black markets and has helped them achieve new dimensions. An example of this is sale of drugs over the internet – an area involving many dubious operators.[56]

Most investigations clearly show that the possibility of earning money has come to be the biggest driving force in cybercrime. Cybercrime targeting organisations or individuals has the same aims as traditional crime, e.g. fraud, blackmail, slander and sabotage. Unlike traditional methods, IT crime is often deemed to be a relatively easy, safe and lucrative way of earning quick money. There are several reasons for this, one being that the criminal can act anonymously. Skilled perpetrators use methods that make it hard to track them down or that leave a trail to the wrong country, organisation or person. Another reason is victims' unwillingness to report such crimes.[57]

The operators behind cybercrime have proven to be both individuals and temporary groups. Knowledge is transferred between individuals – often young people and criminal organisations. This transfer that goes in both directions. The most systematic frauds are largely connected with organised crime of an evidently international nature. These groups have access to extensive resources in the form of advanced tools, botnets and so-called goalkeepers. Against payment, the goalkeepers make their bank accounts available for transactions, and channel the money on from there. They are recruited through social networks or websites, whereby a false company seeks employees. Various specialist functions are brought into play in the organised frauds, recruitment of goalkeepers shifts from one European country to another, and interpreters are hired so as to ensure correct use of language, e.g. for phishing. This crime

[54] According to the Commission, COM/2007/0267, the concept of cybercrime refers to three different categories of criminal activity. The first includes traditional forms of crime such as fraud or forgery, which in this context are committed using electronic communication networks or information systems (below called 'electronic networks'). The second category concerns publication of illegal content using electronic media (e.g. child-pornography material or racial agitation). The third category includes crimes that exclusively target electronic networks, i.e. attacks on information systems, overload attacks and illegal incursion into information systems (so-called hacking). What all of these categories of crime have in common is that they can be committed on a large scale and that there can be a large geographical distance between the criminal act and its consequences.

[55] SIS Terminology for Information Security Edition 3

[56] For further information see: Swedish Medical Products Agency, http://www.lakemedelsverket.se/Tpl/NormalPage 1034.aspx

[57] Read more Chap. 6.2.8.6

can be likened to activity in a criminal business network, where tools of crime, experts and entire criminal concepts are bought and sold. The networks comprise apparently loosely composed cells in which people with the relevant knowledge and ability are temporarily brought in to fulfil a specific function. By using the internet as an interface the operators remain mutually anonymous, and few of them have an overall picture of what is actually going on. It is suspected that the networks can act as hosts for individuals and for small organisations that sell services and products for cybercrime, and that branches of the international organised criminal community control major operations themselves.[58]

The commonest type of information that is stolen is credit-card details and related personal identifying data.[59] The black market for this information is huge, and can be likened to virtual department stores. The stolen information can be used, for example, to buy products on the internet or to take out loans in another person's name. Investigations show that when hacking has taken place it sometimes only takes minutes for the information to be stolen, but it can be months or years before the damage is detected.

5.3.2 Phishing

Phishing is said to be on the increase – particularly in the financial sector. It is said that most phishing attacks target financial operations, and according to some investigations they constitute as many as 95% of cases.[60] There is a trend of less well protected financial institutions increasingly falling prey to this type of crime. New organisations are constantly being affected, and dissemination of phishing is global. It used mainly to be operators in Europe and North America that were affected, but there are now many new phishing attacks on organisations in the Middle East and South America.[61] Another trend is that the attackers are targeting smaller websites for social networks with fewer users, as a result of improved security in the big established websites.[62] Vulnerabilities in internet applications are dealt with in greater detail in Section 6.3.4.

5.3.3 IT-related blackmail

Attention must be drawn to IT-related blackmail, as sources state that blackmailers have often succeeded in getting the money they have demanded.

---

[58] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?,* 2008

[59] Verizon business, *Data breach investigations report*, 2008

[60] See, for example, Symantec Global Internet Security Threat Report, *trends for July-December 2007*, published 2008

[61] Cyveillance, White paper, *Online financial fraud and identity theft report*, 2008

[62] Microsoft Security Intelligence Report January through June 20, An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008, 2008, p. 69
http://download.microsoft.com/download/b/2/9/b29bee13-ceca-48f0-b4ad-53cf85f325e8/Microsoft_Security_Intelligence_Report_v5.pdf

The police cannot confirm this, but it can be deduced from information from IT-security companies. Something that these companies have recently drawn attention to is criminals who get into a company's system and encrypt content in storage media, e.g. information in finance systems, customer registers etc. After a time the criminals contact the company and offer to decrypt the information against payment. As the encryption is strong[63] there seems to be no option but to pay, and this will most probably result in more people adopting this activity.[64]

5.3.4 Viruses and malicious code

Many people deem the biggest risk of major attacks using broad-based internet viruses to be over. Such attacks used largely to be carried out because hackers wished to attract the attention and praise of their peers. The new generation of security threats currently being disseminated comprises harmful attacks carried out by cybercriminals targeting specific companies for personal or financial gain. The methods are getting more and more sophisticated and the perpetrators are becoming increasingly organised and financially motivated. But the threat of broad-based threats should not be totally written off. This was demonstrated in no small way when in January 2009 the Skåne region was infected by a virus which initially infected staff email systems but then spread to medical equipment.[65]

Malicious code[66] can now be bought in customised form for a selected purpose, complete with regular updates and the relevant 'customer support'.[67] There are several instances of companies being affected by targeted mailouts containing malicious code. The malicious code is sent with an enquiry about a meeting or a PDF file whose content appears to concern the recipient's business. It can furthermore be a version of malicious code that the antivirus program cannot currently detect. When the recipient has opened the file a trojan is activated that opens the door to further data espionage, data theft and installation of other malicious code . Norway, for example, has reported an increased trend for targeted trojans during the year. Businesses in the defence sector are said to have been affected, likewise operators in high-tech industries such as electronics, aviation and petrochemicals, but human-rights organisations and managers at various levels have also been hit. Trojans are also used to take control of bank customers' computers.

There are said to be major differences between the various trojans used in this type of fraud. The simplest type can be found free of charge on the internet,

[63] Unlike weak encryption, which can not infrequently be cracked using various aids, correctly used strong encryption is so complex that encryption keys are required to make the encrypted information legible again.

[64] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?,* 2008

[65] Read more in Chap. 6.2.7 regarding vulnerabilities in medical care and healthcare

[66] An umbrella term for viruses, trojans etc.

[67] http://www.ccdcoe.org/8.html

whilst the more sophisticated and expensive versions are less widely disseminated. Vulnerabilities in non-updated software are often used to disseminate malicious code, but it is hard to protect yourself against the more sophisticated trojans, as the antivirus programs and firewalls normally used above all by private individuals do not detect them.

In 2008 there were increased problems with *Drive-by downloads*[68], which meant you could become infected merely by visiting a prepared website. Many users surf using poorly updated web browsers, making them vulnerable to this type of attack.

5.3.5 SPAM

Spam, or unwanted, unsolicited email, continues to be a problem for many businesses. As many as 50% of emails received by a business can be spam. One of the major problems for those affected is not only the quantity per se but also the handling of sudden increases in the volume of various mailouts or junk mails. Handling them necessitates a contingency arrangement, which in turn calls for planning and major resources. Statistics from trade organisations indicate that it is basically a relatively limited group that is behind the majority of spam mailouts.[69] It has proven that targeted, specific measures that have led to success in tracing and shutting off specific botnets that convey spam have resulted in a big, though as yet temporary, decrease in the amount of spam. In November 2008 an unknown internet hotel[70] was shut down following disclosure of information that it had harboured servers for many of the world's spam-sending botnets. It has been stated that in the course of a few hours the quantity of global spam dropped by about 60%. After three to four weeks the levels had by and large returned to normal, but the event shows that it is possible to disrupt distribution of spam and that it is important to investigate the distribution chains so as to find ways of counteracting dissemination of spam.

5.3.6 Social Engineering

Social engineering is manipulation of people using social stratagems to build up confidence that may provide access to sensitive and confidential information.[71] An attack through social engineering has a clear aim, and the target group is limited – unlike the situation with more traditional phishing, where much of the strength lies in achieving a wide area of dissemination so as to increase one's chances. Studies have shown that fraudsters on the internet have become increasingly skilled at manipulating people by using social engineering and exploiting their psychological weaknesses – a successful method. The major difference between social engineering and phishing, which

[68] Read, for example, http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html
[69] Read, for example, http://www.spamhaus.org/
[70] Internet hotel McColo see Report 'Q4 2008 Internet Threats Trend Report', www.halonsecurity.com
[71] SIS Terminology for Information Security Edition 3

is also a form of manipulation, is the greater degree of personal contact that the former entails. Normal security work and individual courses for users and employees are often insufficient to handle this. Theoretical information needs supplementing, e.g. with internal checks and practical exercise, so as to attain the requisite behavioural changes in the staff.

A current Swedish thesis describes the threat as involving a kind of automated social engineering whereby software employing a simple form of artificial intelligence can be similar to human online behaviour.[72] The aim is to manipulate users who do not know with whom or with what they are communicating. This could in the long term lead to problems of confidence in various services on the internet. Several experts point out the importance of paying particular attention to social engineering at a time of financial difficulty when people are possibly more inclined to allow themselves to be deceived by fraud in the form of offers of quick, easily earned money.[73]

5.3.7 Botnets

Botnets are groups of computers that have been infected by malicious code using a control mechanism that allows those behind the botnets to control those computers, often without the users' knowledge. This means that residents of Sweden or organisations may involuntarily take part in criminal activity. It is mainly the number of computers being controlled from one and the same source that makes botnets effective, and they are often used for spam and DDoS attacks.

According to information from many commentators, several million computers have been affected worldwide, but it is impossible to give exact figures in the context. Some commentators think that at least 12 million computers worldwide belong to botnets, with an average of 280,000[74] new computers being connected every day. About 350,000 'zombies' are said to be in daily use, and botnets involving over 5 million hijacked computers have been detected.[75] As described in Section 5.3.5, concerning spam, the number of active botnets decreased for a brief period in 2008, resulting in noticeably fewer spam mailouts.

There are no clear statistics on the dissemination of botnets in Sweden. In a new report the National Post and Telecom Agency (PTS) has estimated that less than one per cent of broadband-connected computers in Sweden are affected. According to Shadowserver, an organisation that specialises in tracing botnets

[72] 'Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks', Marcus Nohlberg, Stockholm University 2009

[73] 'Delete' Newsletter No. 81/08, http://www.darkreading.com/shared/printableArticle.jhtml?articleID=211601123

[74] Halon Security Report, *Q4 2008 Internet Threats Trend Report*, 2009, www.halonsecurity.com

[75] Information from Cyber Warfare conference, Defence IQ PC 2009

and analysing their dissemination worldwide, an average of 1,436 hijacked Swedish computers were noted during the period January to September 2008. In connection with a measurement in October 2008 a Swedish internet supplier stated it had 5,000 hijacked computers in its own broadband network. This would equate to a total of about 27,000 hijacked computers in Sweden as a whole.[76] The information appears to vary.

An operator can rent a botnet to carry out practices such as espionage, sabotage or blackmail. Technical developments have made it possible to update zombie computers with malicious code and new commands several times an hour.

Regardless of a botnet's aims, this often means major handling costs for the businesses affected. The wide range of products on offer is probably the result of the increased demand on a market where anybody can buy or rent a botnet without having any particular skills. The consequences of this are that more and more people have access to the tools required to carry out sophisticated attacks, and there is a risk of more people being attracted to carry out criminal acts.

[76] http://www.pts.se/sv/Document/Reports/Internet/2009/Botnat---Hijacked-computers-in-Sweden---PTS-ER-200911/

6 Vulnerability and risks

6.1 Introduction

This chapter focuses on vulnerability and risks in conjunction with information management. As in Chapter 5, concerning threats, there has been a subdivision of vulnerabilities that have been identified at societal level or at organisational and individual level. At societal level we have chosen to focus on electronic communications, digital control systems, cryptographic functions, the media sector, the public sector, financial services, medical care and healthcare and crime-fighting. They are all characterised by the fact that inadequate information security means an adverse effect on society. Sensitive information can get into the wrong hands, payment streams can be stemmed or rerouted and suspected crime cannot be investigated. The residents of Sweden assume that information management in these areas will function and be secure. Under the heading Organisation and the Individual Level we have chosen to focus on functions that are crucial to the functioning of the businesses of individual organisations or persons. It should be mentioned that a completely unexceptionable subdivision into the societal level and the organisational and individual level is impossible.

All subsections contain a brief description, an account of the importance of vulnerability/risk from an information-security standpoint and from a societal standpoint, assessment of developments during 2008 and discussion of consequences and occurrence. In our opinion, attention should be drawn to vulnerabilities in SCADA systems and the need for secure products and services.

6.2 Societal level

6.2.1 Electronic communications

All sectors of society are affected to some extent if electronic communications fail. Electronic communications and the electricity supply are both crucial to maintenance of a normally functioning society. Businesses often run on electricity, whilst they are governed and controlled by means of electronic communications. Creation of redundancy for electronic communications is complicated, as the operators often rent capacity from each other.[77]

[77] KBM, *Will we cope with the crisis? Society's capacity to deal with an emergency 2007*, KBM's educational series 2008:2. The report analysed both electronic communications and the electricity supply in detail, and several deficiencies were noted. http://www.krisberedskapsmyndigheten.se/upload/17065/klarar_vi krisen_temaserien2008-2.pdf

In autumn 2007 and spring 2008 PTS carried out planned supervision of functionality and technical security in service providers in the fields of telephony, mobile telephony, IP telephony, the internet, network capacity, fixed mobile, email and TV.[78] In this context security means work on preventing interruption and disruption by means of risk analyses and risk management, planning for handling of interruption and disruption, and follow-up when they occur.

PTS's general advice is that security work should be decided on at management level and should be followed up in the business. The supervision shows that this takes place in nine out of ten service providers, both under normal circumstances and in the event of extraordinary occurrences. Not everyone, however, follows up on implementation of the measures decided on. The biggest deficiency in security work is stated as being the lack of *documented* procedures. Documented procedures are required in order to ensure that security work is continuous and systematic – more uniform and less dependent on individuals. Some service providers see security work as activities connected with technical infrastructure, but the present stipulations apply to all operators providing electronic communication networks or services, regardless of the technology. PTS points out the importance of including the soft factors such as *staff, skills* and *processes* in the security work. They are otherwise easily forgotten in the context, even though they very much contribute to the successful functioning and technical security of the services and networks. It is important to inform users of *upgrades* and *changes*, as they can affect operational security and thus users' chance of using electronic communications services. In spite of this, two out of ten providers fail to notify their customers of such changes.[79]

6.2.2 Digital control systems

During 2008 the non-specialist press began in earnest to detect that vulnerabilities in digital control systems (SCADA) were also being reported. The first actual SCADA vulnerability was reported by US-CERT in May 2006, and since then 23 specific SCADA vulnerabilities have been documented and reported. Most of the vulnerabilities are what in the traditional IT world would be considered relatively common vulnerabilities, e.g. of the buffer overflow type. IT security in SCADA systems is often deemed to be 5-15 years behind the traditional IT world. The following example attracted great interest, both in the specialist press and in other media, and clearly illustrates the lack of good processes for reporting and handling vulnerabilities.

[78] The aim of the supervision was to follow up adherence to the stipulations regarding good function and technical security in accordance with the Swedish Electronic Communications Act (LEK)

[79] Good Function and Technical Security in Electronic Communications - PTS-ER-2008:13

Example (Vulnerability in CitectSCADA)

One of the highest-profile events of 2008 is the reporting of a vulnerability in CitectSCADA.[80] At the end of January the security company Core Security Technologies detected a vulnerability in the software and contacted Citect's support.[81] The subsequent process took over five months, and initially Citect saw no need to prepare an update (patch) beyond the normal upgrading of the system. Citect only developed a patch after Core had postponed the publicising of the vulnerability three times and had involved CERT organisations in Australia, the USA and Argentina. On 11 June 2008 'CORE Security advisory CORE-2008-0125' was released. Citect encouraged its customers to upgrade the system, but in a press release it played down the gravity of the security hole. On 5 September 2008 an attack code (exploit) was released that exploited the vulnerability, in the form of a module for the publicly available attack packet Metasploit. Shortly afterwards Citect amended its initial press release and emphasised the gravity of the security hole.[82]

There are a number of factors that make the CitectSCADA example interesting. First of all it may be worth noting that Core Security Technologies is not a traditional SCADA consultancy, and that this is thus an example of how the problems are beginning to get more and more interesting for people other than the specific suppliers and users in the SCADA industry. The vulnerability in the software was of the buffer-overflow type, and could, if exploited, lead to an unauthorised person being able to close down the software (a DoS attack) or execute their own code in the system. Availability in SCADA systems is critical, and even if an attacker fails to take control of a business controlled by the program, a DoS attack can have serious consequences. As Core has documented and publicised all its contacts with Citect, the actual course of events can be studied in great detail. The example can thus also be seen as an illustration of the fact that many SCADA suppliers lack the processes to handle and report on vulnerabilities. Citect did not initially consider it necessary to develop a patch, and the company only changed its mind after Core had repeatedly exerted pressure and stated that they were serious about publicising the vulnerability. Core also made repeated attempts to get Citect to give a date for when a patch would be ready, but Citect delayed this a number of times – in part by asserting that it was an in-house, commercial decision. It is also worth noting that throughout the process Citect's email communications with Core were unencrypted. The company did not have the option of using ordinary

[80] Citect Pty Ltd has been owned by Schneider Electric since 2006, and supplies software for industrial automation in over 80 countries through a network of over 500 partners. CitectSCADA is an HMI/SCADA program package run on standard personal computers using Microsoft operating systems http://www.citect.com/index.php?option=com_content&view=article&id=1457&Itemid=1314

[81] http://www.coresecurity.com/content/citect-scada-odbc-service-vulnerability

[82] http://www.citect.com/documents/news_and_media/CitectSCADA-security-response.pdf

encryption such as PGP. The course of events that followed the reporting the vulnerability is also very interesting.

After Citect had played down the gravity of the vulnerability in their press release, an exploit written for the attack packet Metasploit was released – the first public exploit code to directly target SCADA systems. The publicising of the exploit code was followed by considerable debate in SCADA circles. It is important, however, to bear in mind that the vulnerability per se was fairly simple, and that in the traditional IT world exploit code of this type for easy-to-use attack packets such as Metasploit is released every day. A considerable amount of non-public exploit code has been seen over the past two years, according to well-known consultancy companies such as Digital Bond, and many experts have thus expected public exploit code targeting SCADA to come sooner or later.

There is currently no information on whether any users have been affected by an incursion as a consequence of the vulnerability in CitectSCADA. Neither is there any information on how many users have actually installed the patch released by Citect. Many users still lack procedures for system upgrades, and many SCADA systems also lack antivirus and intrusion detection systems (IDSes). In recent years, however, more and more specially produced hardware – e.g. firewalls that recognise protocols used in SCADA systems – has come onto the market. Changes are also beginning to be discernible in the field of software. There are currently around 25,000 plug-ins to Nessus, which is the commonest program for scanning for a specific vulnerability. Currently 40 of these plug-ins are specifically related to SCADA systems. Since ordinary IT components are much used in SCADA systems, many traditional Microsoft and UNIX vulnerabilities are also critical for SCADA systems.

KBM's situational assessment of societal information security for 2008 reported on the CIA's presentation regarding a number of attacks on SCADA systems.[83] The presentation did not include any specific technical details or information on the types of attacker in question. The presentation was not followed up in 2008, and the information is far too scant for it to be of any practical use to users of SCADA systems. The lack of openness about incidents continues to be a problem in the field, and in conjunction with the increased interest from the non-specialist press that followed the vulnerability reports, several old incidents have again been taken up by the media. Few new incidents were reported in 2008, though the following describes an incident that attracted great attention and that particularly illustrates the problem of integrating SCADA systems with administrative IT systems.

Example (Disturbance in Edwin I. Hatch Nuclear Power Plant, Unit 2)
On 7 March 2008 the Hatch 2 nuclear reactor in the USA was forced to implement a rapid shutdown following a software update in a computer in the plant's office network. After 48 hours the plant was able to start up again. The computer that was updated monitored chemical and diagnostic

[83] At the SANS SCADA Security Summit conference in New Orleans in January 2008.

> data from the plant's primary control systems, and the software was designed to synchronise data in the primary control system with data in the computer in the office network. When the computer in the office network was restarted, data in the control system was adjusted, and the plant's security system interpreted this as a possible reduction in the water reservoir in the reactor's cooling system. Thus the plant's security system worked correctly, and according to information in the incident report submitted to the US Nuclear Regulatory Commission (NRC) the plant's security was not affected.[84]

Integration of SCADA systems with office networks is continuing, and cannot be halted – neither should it be. The guidance on increased security in digital control systems in critical infrastructure[85] drawn up in 2008 by KBM and a number of authorities in collaboration with the industry recommends that the integration be controlled. For certain types of extreme critical system, however, the only solution may be complete isolation of SCADA systems from other networks.

6.2.3 Cryptographic functions

Information should be protected during handling and storage, and in communication between organisations. Cryptographic functions can be used to guarantee confidentiality, integrity and availability.

When an organisation is to introduce cryptographic functions this should be well supported throughout the organisation, from management to end user, as it is important that resources be available in the form of the means and the staff to develop, introduce and administrate the cryptography to be introduced. The end users must also be informed, trained and given access to instructions for use. The technology only constitutes a small part of a secure solution involving cryptographic functions. The greater part comprises regulatory frameworks, procedures, training and active staff participation. These components must be developed and made known within the organisation. Attackers who are planning to attack systems that use cryptographic functions will first look at the regulatory framework in order to find weaknesses in procedures and in handling of cryptographic keys or certificates. Deficiencies in the end user's training or understanding of the importance of adherence to instructions for use and set procedures make it easier for the attacker to carry out a successful attack.

Vulnerabilities do not only arise in implementation – it is also important to choose the right cryptographic function. In the public sector there are currently

---

[84] There is currently no official report from NRC on the incident. The above description of the course of events is taken from the Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html, which interviewed representatives of the company in charge of technical operations at the plant.

[85] http://www.krisberedskapsmyndigheten.se/upload/17913/SCADA_sv_2008.pdf

no comprehensive guidelines on choice of cryptographic function, and this can lead to a lack of security. The plan of action for societal information security proposes drawing up general advice and recommendations aimed at government authorities, municipalities, companies etc. The aim is to achieve a security level that will facilitate exchange of information between authorities and various functional systems.[86]

6.2.4 The mass media

The news media carry out societally important operations in several respects – both under normal circumstances and in the event of extraordinary occurrences. The media are included in society's warning, alarm and information system. Parts of the mass media are thus very important for raising the alarm and for crisis management in the event of extraordinary occurrences – both for the dissemination of information and for decision-making in society as a whole. Important communications to the general public (VMAs), official messages and nuclear alarms are examples of important information systems that are in various ways dependent on well-functioning media channels.

From a democratic standpoint the media are necessary as a daily source for our monitoring of outside events, for free speech and for opinion-forming. The fact that the general public expect constant access to their normal information sources is noticed as soon as there is an interruption.

Power cuts, interruption of electronic communications and threats to journalists are the three threats that big companies take most seriously. After fire, power cuts and interruption of electronic communications are the events that are deemed to entail the most serious consequences.

Hitherto only 'blue-light' authorities such as the police and the emergency services have been connected to the RAKEL system[87], but the group of users will increase, and the media companies have expressed a need to connect particularly affected media to the system. RAKEL can be used, for example, to convey VMAs by safeguarding the communication between the Swedish emergency-services provider SOS Alarm and Swedish Radio.[88]

Digital TV switchover has changed the conditions for dealing with disturbances and using alternative distribution routes. Technical systems are often vulnerable in conjunction with major changes. The shifts in technology mean a renewed need for learning, and may have an adverse effect on security and contingency arrangements during a transitional period. A crucial party in the

[86] Plan of Action for Societal Information Security, p. 49

[87] RAKEL is a common radio-communications system for organisations in society working in the field of general order, security or health. As from 1 January 2009 MSB has been responsible for RAKEL's operations.

[88] National Board of Psychological Defence, *Risk and Vulnerability Analysis of the Media Sector 2008,* 2008, p. 23

media sector is Teracom, who own and are responsible for the digital and the analogue terrestrial TV and radio networks. Even though Teracom has nearly ten years' experience of digital broadcasts, its experience of improvising solutions in a crisis is not yet as extensive as its experience in an analogue environment.

PTS has decided that Teracom is under a general obligation to give other parties access to the terrestrial network. The consequences of this are currently hard to assess. During 2008 the Ministry for Enterprise, Energy and Communications commissioned an investigation into the consequences of selling the state-owned company Teracom. A sale should be preceded by a thorough analysis of the possible consequences for Teracom's security and contingency work from a societal standpoint.

6.2.5 The public sector

6.2.5.1 Continuity planning

The work on situational assessment involved an investigation into the handling of continuity planning in municipalities. Major deficiencies were demonstrated, the biggest being related to the planning of businesses' work on counteracting unplanned interruptions and on their behaviour in such an eventuality. Deficiencies in municipal continuity planning have also been revealed in the ongoing work that has been carried out by KBM and MSB, for example during active support from the authority in driving the planning process forward, and regarding the information-security training provided by the county administrative boards for the municipalities.

The municipalities for the most part have *policy documents* containing defined responsibilities and guidelines regarding implementation of the work on information security, though as a rule the policy documents provide no direct guidance on the scope of continuity planning. In no instance has management stated that there are particular reasons for preparing an emergency plan, and there are usually no plans for coordination of continuity planning amongst management, operations and IT support. Responsibility for dealing with interruptions clearly lies with line organisation, but at the same time there is no insight into the dependency of internal operations on IT support. Various responsibility roles regarding information security have been defined, but in several instances their significance is unclear, particularly with regard to the system-ownership role.

The municipality must also function in the event of a disturbance in the form of an interruption. It is thus important to identify which operations in the municipality are absolutely necessary, so as to be able to avoid unacceptable consequences for the residents of Sweden. In most municipalities the planning process for handling of interruptions has started. Established and set acceptable operational *interruption times* are crucial initial values for continuity planning with regard to the municipality's most important IT systems. These values are lacking in many of the municipalities investigated. Calculation of interruption times is based on the service level to be maintained in the event of an interruption, critical points in time and how the extra work

accruing after an interruption is to be handled. In certain instances interruption times have been determined without these initial values.

Planning of how operations could be carried out in the event of an interruption using various information-management *backup procedures* is lacking throughout. The work has not started or been carried at any of the ten municipalities visited. The lack of backup procedures means that unplanned interruptions could greatly reduce the service level of several important societal functions in the municipality. The consequences of an interruption may be more serious at certain times. Any decision on the service level's acceptability will depend on an assessment of the viability of operational backup procedures.

At *IT/operational level* the prerequisites for handling an interruption usually exist. The weaknesses are a lack of coherence and updating in existing system documentation and difficulty dealing with dependence on individuals. Continuity plans are in most instances at IT/operational level, though they are not coordinated with operational requirements where the requisite initial values from operations are lacking.

There are major difficulties in keeping planning up to date and in achieving *continuity* throughout the planning process. In the municipalities visited the process has in several cases started but has gradually lost momentum. Repeats in the planning then take place, and in many instances this leads to previous experience and knowledge not being taken into consideration in the planning process.

6.2.5.2 Other administrative and technical vulnerabilities

A survey-based investigation aimed at authorities indicates greatly varying levels of information security in the survey subjects, e.g. regarding information-security policy, threat analysis, incidents and handling of log data.

Small authorities more often lack *information-security policy* than big ones. Several authorities stated that they had an IT-security handbook, IT-security instructions or an IT-security policy, but no overall information-security policy.

Of the 73 authorities who responded to the survey, 71 per cent stated that they are preparing *threat analyses*.

Several incidents were reported, including copyright crimes, attempts to hack into IT systems, computer hacking, DoS attacks, viruses, trojans, botnet infections and various instances of malicious code . Other types of event also occurred, e.g. temperature increases and power cuts in computer halls, incomplete backup of most systems and user data, and threats to staff.

68% of the authorities who responded to the survey stated that they gather and store log data, though only 32% stated that they continuously analyse this data.

Many authorities state that they might report incidents to Sweden's IT incident centre SITIC, for which PTS is responsible.

6.2.6 Financial services

For society it is of the utmost importance that the payment system feature a very high level of operational security for financial societally important services. The core of the payment system is made up of the clearing system for major payments (RIX), the bank-giro system, the Swedish Securities Register Centre (VPC), Data Clearing[89] and the big banks' links to the systems. According to the Swedish Financial Supervisory Authority (FI) it is as a rule only disturbances in the four major banks and the central financial-infrastructure companies that could put society's basic financial services out of action. According to FI, disturbances in small local bank branches, small financial companies, individual card terminals and ATMs are negligible from a societal standpoint.[90]

Only a few payments in every thousand are currently cash payments, whilst the rest are handled using computerised infrastructure that interconnects various financial operators.[91] Damage to the payment systems and financial services may have serious consequences for the social economy and could in the long term affect confidence in the entire financial system[92]. In the absence of legal requirements binding companies to maintain a minimum of operational security for payment services, FI is working on broadening the collaboration to include sectors beyond FI's area of responsibility such as authorities and companies in the electricity, telecom and internet sectors.[93]

FI only has supervisory responsibility for certain parts of the payment system. RIX, card readers, transportation of items of value and some parts of card-payment clearing are examples of areas for which FI is not responsible. There are also parts of the payment system that are outside Sweden and that are subject to the supervision of foreign authorities or are not supervised at all.[94]

A significant part of financial infrastructure is now also made up of the general public, who communicate with internet banks through private computers.

---

[89] Data clearing is a system for conveying payments from account to account. Bankgirocentralen AB manages operation and the Swedish Bankers Association owns the system. During 2008 over 99 million transactions were conveyed. http://www.bankforeningen.se/Publicerat/Nyhetsbrev/Nyhetsbrev%20nr%201%20februari%202009/Drygt%2099%20miljoner%20transaktioner%20i%20Dataclearingen.aspx?tipsa=true

[90] Swedish Financial Supervisory Authority report 2008:10, *Responsibility for the Payment System*, p. 3.

[91] Swedish National Bank (Sveriges Riksbank), *Vulnerabilities in the Modern Payment System,* Srejber, E. Speech at Swedish Security Assembly in Eskilstuna 18.10.2006.

[92] Swedish National Audit Office, *Emergency Preparedness in the Payment System*, RiR 2007:28

[93] 'Responsibility for the Payment System', Swedish Financial Supervisory Authority report 2008:10, p. 1.

[94] 'Responsibility for the Payment System', Swedish Financial Supervisory Authority report 2008:10, p. 4.

When private individuals become part of the financial infrastructure, this complicates the security work that is otherwise carried out in financial institutions and government authorities.[95] Frauds targeting users of internet-banking services are a common cybercrime. The fraudsters exploit deficiencies in private individuals' security systems or in their security awareness, thus gaining access to the data they need for use of personal internet-based financial services, e.g. carrying out transactions and trading in securities.

The combined loss as a result of frauds can involve significant amounts, and can mean damage to confidence in internet-based financial services. A problem in combating organised fraud is that it is hard to achieve a holistic approach, as each individual case is treated individually.[96] With individual crimes that attract a low sentence, the police are not able to use secret telephone surveillance in their enquiries and for investigation of the frauds, as the Code of Judicial Procedure states that telephone surveillance presupposes a minimum sentence of six months' imprisonment.[97] In these instances, neither is it possible to ask operators for IP addresses, as the Swedish Electronic Communications Act only permits disclosure of such data if there is a suspicion of crime for which a minimum sentence of two years is prescribed.[98]

Another problem is the international nature of the frauds dealt with in Section 6.2.8.4. on cross-border collaboration.

6.2.7 Medical care and healthcare

Electronic healthcare records constitute a crucial part of healthcare information systems. They contain sensitive information in many forms, which must be given appropriate protection, not least for legal reasons. On 1 July 2008 the new Patient Data Act came into force, facilitating full implementation of the national IT strategy for nursing and healthcare, which was presented in 2006. The aim is to use IT to achieve better collaboration between parties in the field of medical care and healthcare and improved patient orientation regarding healthcare activities. It is very important that patient information, which is divided up amongst various sections of the health system, can be transferred securely, so as to guarantee and maintain a decent level of patient care and in order to ensure patient integrity.

But over the years Swedish healthcare has been affected by several serious IT failures and system errors[99] – chiefly incidents in connection with case-record systems that have crashed and made patient records unavailable. According to a thesis on information security within the healthcare sector, one of the biggest

[95] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008 p. 21.

[96] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 29.

[97] Code of Procedure (1942:740), 27 Chap. Section 19

[98] Electronic Communications Act (2003:389) Chap. 6 Section 22 p. 3

[99] See, for example, Computer Sweden's compilation of the Swedish health system's IT crashes and system errors in 2008. See http://computersweden.idg.se/2.2683/1.213345/ett-ar-av-haverier-och-it-problem

security problems is non-availability of patient information when it is required.[100] For example, in January 2008 a power cut at Lund University Hospital led to the electronic case-record system being put out of action for three hours. Hospital management assessed the disturbances as being very serious, and an emergency situation was nearly triggered. In January 2009 a virus in the Skåne Region rapidly spread to medicotechnical equipment through the region's internal email system.

The media have also reported on deficiencies revealed in conjunction with penetration testing of the county councils' security systems. In one instance it became possible to access Apoteket AB's prescription-management system, which in practice means that prescriptions could have been issued.[101]

The thesis on information security in the healthcare sector draws attention to a number of instances where measures are needed. With regard to *technical security*, it is very important to review and improve handling of verification, authorisation and signing. Tools for log management, open access, problems of integration between different systems and the lack of encryption for sensitive information need to be discussed. Within *administrative security* the main problem is the lack of guiding legal and organisational documents on handling of information and clear work procedures for this. By creating policies for information security and IT strategies, training staff and performing risk and vulnerability analyses you can highlight issues and meet needs.[102]

6.2.8 Fighting crime

6.2.8.1 Background

Cybercrime[103] currently constitutes a serious threat to societal activities. National crime-fighting faces a number of challenges, in particular bearing in mind that it must counteract and deal with crime that is global and recognises no borders. A characteristic of cybercrime is that it can be committed on a large

[100] Rose-Mharie Åhlfeldt, *Information Security in Distributed Healthcare,* Stockholm University & University of Skövde, 2008.

[101] *Healthy Technology, IT in Healthcare*, http://itivarden.idg.se/2.2898/1.212950/latt-att-hacka-sig-in-i-landstingsnat

[102] Rose-Mharie Åhlstedt, 2008, p. 62.

[103] According to the Commission, COM/2007/0267, the concept of cybercrime refers to three different categories of criminal activity. The first includes traditional forms of crime such as fraud or forgery, which in this context are committed using electronic communication networks or information systems (below called 'electronic networks'). The second category concerning publication of illegal content using electronic media (e.g. child-pornography material or racial agitation). The third category includes crimes that exclusively target electronic networks, i.e. attacks on information systems, overload attacks and illegal incursion into information systems (so-called hacking). What all of these categories of crime have in common is that they can be committed on a large scale and that there can be a large geographical distance between the criminal act and its consequences.

scale and that there may be a big geographical distance between the criminal act and its consequences.

Deficiencies in countries' national fighting of cybercrime and legislation are exploited by the organised criminal community. Unlike crime-fighting authorities, those who commit cybercrime are not bound by legal and geographical boundaries. Individual states must word their descriptions of crimes identically if functioning and efficient international regulatory frameworks and conventions are to be created.

If these crimes are to be efficiently prevented and if nations are to be able to legislate against them, the measures required must be based on an international, cross-border approach. International agreements such as the Council of Europe's Convention on Cybercrime[104] are no more comprehensive than the states that ratified[105] the Convention.[106] The need for international measures in the field has also been identified within the EU, and in 2007 the Commission adopted a general-policy initiative to improve coordination at European and international level with regard to combating cybercrime.[107]

The objectives of the EU's initiative are as follows:

- To improve and facilitate coordination and collaboration between the authorities who are combating cybercrime, other affected authorities and other experts within the EU
- To develop a consistent political framework for the EU in its fighting of cybercrime, in coordination with the member states, affected EU bodies, international organisations and other affected parties
- To increase awareness of the costs and risks that cybercrime entails.

International experts[108] point to three conclusions that are adversely affecting the crime-fighting:

- States are not taking IT crime seriously,
- The cross-border work is not being sufficiently prioritised by nation states, and

[104] Council of Europe Convention
http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[105] A decision by a legislating assembly to approve an agreement or a treaty, and often used regarding approval of international agreements and conventions.

[106] Swedish National Defence College, Nina Wilhelmsson *International-law aspects of cyberthreats and protection against information operations,* 2008, p. 14

[107] COM(2007) 267 Communication from the Commission to the European Parliament, the Council and the European Union's Regional Committee, Introducing a general policy for the fight against cybercrime
http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=sv&type_doc=COMfinal&an_doc=2007&now_doc=267

[108] Compilation to be found in *McAfee's Criminology Report,* 2008

- The skills of the crime-fighting authorities are insufficient for handling of the crime.

We have chosen to focus on the need for harmonised international legislation, international law and information operations, cross-border legal and police collaboration, skill-enhancing IT training for crime-fighting authorities, and the hidden statistics on reporting of cybercrime.

6.2.8.2 Legislation

Individual states must use identically worded descriptions of crime if functional and efficient international regulatory frameworks and conventions are to be created. The lack of harmonisation is creating difficulties with regard to the possibility of extradition, prosecution and jurisdiction between states.

The Council of Europe's 2001 Convention on Cybercrime includes regulations on the penal process and a system of international collaboration for states that have ratified the Convention. 46 states, both within and outside Europe, have signed the Convention, but thus far only 23 have ratified it.[109] Sweden is one of the countries that have not yet ratified the Convention. Efficient international collaboration is facilitated by a joint regulatory framework, and the fact that so many countries still have not ratified the Convention on Cybercrime means it has not yet gained full impact.

The Convention on Cybercrime is criticised in some circles as being too dependent on technology. Now-common cybercrimes such as phishing and identity theft did not exist when the Convention was drawn up, thus it provides no guidance on combating and collaborating against these types of crime.[110] The difficulty with formulating technology-dependent laws is that they often quickly become outdated and old-fashioned, thus the legislators are required to write laws that are less dependent on technical specifications. However, such technology-independent legislation instead risks becoming general and thus providing less guidance on handling of specific situations. Overall this indicates a complex problem.

6.2.8.3 International law and information operations

Looking at information operations from a legal standpoint, the 1945 United Nations Charter regarding international peace, security and international law is of particular interest.[111] International law regulates the relationship between

---

[109] See http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=7&DF=2/27/2009&CL=ENG

[110] McAfee *Virtual Criminal Report 2008*, p. 20.

[111] Legal regulations between states and organisations. When international custom (states' common mode of action – practice) is accompanied by states' legal conviction that current law is reflected by customary practice, one speaks of general international law or common law.

states and the law on warfare. The general prohibition of force means that a state can only resort to self-defence in the event of armed attack or if use of force has been authorised by the UN's security council. If any of these criteria has been met it is still necessary that a countermeasure (counterattack) be deemed *necessary*, be *proportional* and take place *immediately*. The law on warfare is regulated by humanitarian rights, which prohibit specific attacks on civil targets (e.g. information infrastructure for electricity and water supply) in accordance with the distinction principle.[112]

Problems arise when you redefine tried-and-tested expressions such as armed attack and traditional weapons.[113] *'The speed and technical complexity of cyber activities requires prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks.'*[114] Technical developments create new requirements regarding conventions in the field of international law, in particular with regard to the principle of protecting the civilian population in the event of armed conflict and the work of limiting methods of warfare.[115] Unlike traditional warfare, IT allows a small group or even an individual to attack a state. The UN Charter and international law are only applicable where a state is behind information operations.

Thus from a legal standpoint the information operations against Georgia and Estonia are a grey area. The lack of an obvious aggressor and the fact that the attacks did not cause any tangible human suffering mean that it is not possible to use the international regulatory framework for armed conflicts[116] to get at the perpetrators. The sovereignty principle enshrined in international law thus makes it hard for a country that has been subjected to cyberattacks to follow up electronic trails beyond the country's borders, as international law is based on states' and organisations' attitudes to each other.[117]

In a speech to the UN General Assembly in September 2007 Estonia's president called for a joint UN convention against cyberwarfare and cyberterrorism. A debate is also in progress within NATO on giving information operations the same status as attacks on a country's sea, air or land boundary in accordance with Article 5 of the North Atlantic Treaty[118], which obliges the NATO countries to collaborate and provide mutual assistance in a situation in which one or more member countries are subjected to attack. Discussions within NATO, however, indicate that such collaboration is unlikely, bearing in mind the difficulty of assessing where a cyberattack has originated.

---

[112] Nina Wilhelmsson, p. 13.

[113] Nina Wilhelmsson, p. 7

[114] Sofaer, Abraham D. & Goodman, Seymor E. et al. (2000) *'A proposal for International Convention on Cyber Crime and Terrorism'*, CISAC Report, August 2000.

[115] Nina Wilhelmsson, p. 7

[116] Law of Armed Conflict, (LOAC)

[117] Nina Wilhelmsson, p. 12.

[118] http://www.NATO.int/docu/basictxt/treaty.htm

6.2.8.4 Cross-border collaboration

The risk of not having any well-functioning cross-border collaboration is that attention is not drawn to the scope of cybercrime and the systems behind it. National police forces on their own can seldom carry out comprehensive investigation of cybercrime. Difficulties getting legal assistance from certain countries in practice mean that fraud must be handled within Sweden, even though both the servers and the operators may be elsewhere in the world. The consequence is a hunt for goalkeepers[119] without any great chance of catching the organisers or investigating the systems behind the crime.

The police are also finding it hard to gain an overall national picture of cybercrime. The reason for this is that it is hard to coordinate the local police authorities' information on the different cases. There is thus a risk of missing the scope of certain crimes and the systems behind them.[120] With the aim of getting an overall picture of cybercrime the organisational structure must thus be handled using independent county-police authorities.[121] There have been examples of banks notifying police of common patterns behind crimes in various parts of the country, whereupon the police have coordinated the investigations of these crimes at a police authority, leading to positive results.

6.2.8.5 Training

Knowledge of the field is very important to protection against cybercrime. IT as a means to criminal activity and a target for it is a relatively new phenomenon, and has resulted from general technological developments.

Sources indicate that the biggest gaps in knowledge in the judicial system are to be found within the courts and amongst defence lawyers.[122] Particular attention has been paid to the handling of IT-related evidence.[123] Increased specialisation in the legally/technically/financially complicated types of target would indubitably lead to greater knowledge amongst the judges in the legal area in question and thus to better-quality implementation of the law. It would probably also lead to increased efficiency, which in turn would lead to faster court settlements regarding these types of target. Specialisation in legally/technically/financially complicated types of target would thus lead to better meeting the demand on the part of the residents of Sweden for quality and speed in sentencing operations.[124]

---

[119] See Section 5.3.1

[120] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 67.

[121] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?,* 2008, p. 29.

[122] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?,* 2008, p. 53.

[123] For example the ADBJ seminar on 16 October 2008
http://www.adbj.se/adbjweb/events.php?op=read&id=96

[124] Swedish National Courts Administration (DV), *A preliminary study in collaboration with the Swedish Association of Judges.* DV report 2003:3, p. 30.

The investigation 'The Police of the Future' includes strategic analysis by the Swedish National Council for Crime Prevention (BRÅ) with regard to organised crime, identifying a number of trends that can be assumed to be of significance to societal development and police operations. One trend is deemed to be an increase in new crime as a result of technical developments.[125] Another trend will be a clearer call for specialisation and for police officers with specific expertise.

6.2.8.6 Unrecorded cases

There is little tendency to report cybercrime to the police, thus crime-fighting authorities have difficulty finding out about the scope and nature of cybercrime. The paucity of reports also makes it difficult to emphasise the need for crime-fighting resources.[126]

Businesses sometimes handle events internally as technical problems, whilst they are actually being subjected to cybercrime. Security work and crime-fighting in the field of IT is an area in which private companies are taking up an unusual amount of space and are assuming an unusually high level of responsibility. A problem arising from this role distribution is that the boundaries between crimes and incidents are becoming blurred and that the formal crime-fighters are losing their overview of cybercrime. Certain types of crime such as blackmail are only handled by IT security companies and do not usually come to the attention of the police.[127]

Companies and organisations that have been subjected to cybercrime are reluctant to report it. There are several explanations for this, one being that they are afraid of negative publicity, that they blame themselves for the lack of security and that they wish to avoid damaged confidence in their company or organisation. Another contributory reason is the perception that the police lack the resources and capacity to investigate the crimes. The investigations take a long time, and the end result is often perceived as being poor.

Fear and threats of reprisals also figure as reasons for companies biding their time or completely refraining from reporting matters to the police. Fear of reprisals is an unusual reason to refrain from reporting crime to the police, and is reminiscent of the reaction of victims of crime and witnesses who have been subjected to or have witnessed crimes committed by the organised criminal community.[128]

[125] Swedish Official Government Report SOU 2007:39, *The Police of the Future,* p. 101.
[126] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 57.
[127] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 52.
[128] BRÅ/KBM, *Cybercrime and Incidents – A Threat to Critical Infrastructure?*, 2008, p. 59.

6.3 Organisation and the individual level

6.3.1 Mobile units

Thanks to rapid developments, mobile phones, USB memory sticks, MP3 players and portable hard disks can now handle a large amount of information and, in particular in the case of mobile phones with operating systems, offer a number of services that would previously have required access to a computer. The increased number of areas of application and the increased capacity not only constitutes a form of support for businesses but also presupposes resolution of a number of security issues.

A business's *internal handling* of mobile units often displays deficiencies. USB ports are usually not blocked, making it easy to connect a USB memory stick containing malicious code to the organisation's computers and networks. Furthermore, USB memory sticks and portable hard disks are both portable and have a high capacity, making it easy to steal large amounts of information. Laptops also constitute a security risk, as they often lack hard-disk encryption and are easy to steal. Things are also moving towards transfer of more and more services and information to mobile phones[129] and other mobile units such as PDAs, thus imposing stringent security requirements.

With regard to *external threats*, international studies indicate an increased risk of mobile phones being subjected to text-messaging spam, viruses and botnet attacks during 2009.[130] In particular, increased use of mobile phones for financial services will contribute to attacks becoming more targeted and frequent. The increased usage and changed threat to mobile units make it extremely important to ensure that these units are also covered by the organisation's security policy and security culture. Organisations currently often fall short in their handling of mobile units.[131]

The use of mobile broadband is growing. Technical security in electronic communications systems in mobile broadband is relatively good. There is currently no known or predicted way of obviating security (cracking the encryption) in 3G networks (UMTS), and security in 2G networks (GSM) is so high that attacking these networks requires expensive equipment and manpower.[132]

[129] In particular so-called smart phones

[130] See, for example, Georgia Tech Information Security Center, *Emerging Cyber Threats Report for 2009*, http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

[131] http://www.atea.se/default.asp?ml=6796&naar=&p=5141

[132] PTS Report More Secure Wireless Communication (coming out in April 2009)

6.3.2 Wireless LAN

Unprotected wireless LAN, i.e. using unencrypted traffic, has long been seen as entailing a potential lack of security.[133] There are two main threats to wireless communication: interception of traffic and unauthorised access to the wireless network.[134]

More and more people are using their home network for banking[135], buying and selling products and services, and tending to private matters concerning children, school and healthcare. There is also an unknown number of people who at least to a certain extent work from home[136], connected through a wireless network. Unprotected networks mean that a great deal of sensitive data can relatively easily be intercepted. As we are heading for increased use of the internet for a number of different services, unprotected wireless networks constitute a risk.[137] One of the biggest risks is outsiders gaining access to the wireless network and exploiting it for criminal purposes, e.g. stealing information, intercepting log-in details and downloading illegal material.[138]

In autumn 2008 KBM commissioned an investigation with the aim of gaining greater insight into the number of wireless networks and use of encryption. The results of measurements show that the majority of private networks are encrypted but that many are still unprotected. In all three locations where measurements were carried out[139] 26% of the wireless networks did not have encryption switched on. To judge by the networks' names they are largely owned by universities and hotel and conference facilities. Just as with teleworking, it can be assumed that wireless networks in hotel and conference facilities are to a large extent used to handle company or official information that may be sensitive. There are various ways of using a portable client to set up various forms of communication encryption – using encrypted email for example. Most VPN solutions available on the market provide excellent protection for this type of communication. Awareness of the need for this type

[133] It should also be mentioned that unencrypted wireless LAN often features protection in the form of log-in measures and other measures. The efficiency of the protection depends on the measures and threat.

[134] The regulatory changes based on the IPRED directive may change the threat with regard to utilisation of unprotected wireless LAN. See further 4.8

[135] They usually take place, however, using encrypted connections, and are thus well protected against bugging.

[136] Here, too, companies usually provide solutions (various VPN solutions) affording satisfactory security

[137] PTS has drawn up a report on security in local wireless networks with advice for users (PTS-ER- 2007:16) See also PTS Report More Secure Wireless Communication (coming out in April 2009)

[138] The amended legislation with regard to investigation of suspected illegal download of copyright-protected material may alter the threat and create an increased incentive to use someone else's unprotected network to download material. See Chap. 4.8

[139] Stockholm, Gothenburg and Malmö

of security solution is, however, very important, though the users display shortcomings.[140]

As protection against interception, use of the WPA2 encryption protocol can be a relatively good solution that should be sufficient for average domestic use for private purposes, though the WEP encryption protocol is still used to a certain extent for encryption. The protection provided by WEP cannot nowadays be deemed to be as good, and for several years now WEP has not been included in new equipment. It is important to be aware of the limits of encryption protection – for example, use of WEP can lull users into a feeling of false security.

Bluetooth is another wireless device that suffers from security defects. The technology is cheap and implementation is complex, thus leaving plenty of scope for attackers to develop various types of attack by trial and error. As Bluetooth technology is now beginning to be used in increasingly sensitive equipment, e.g. in the field of medical care and healthcare, the vulnerabilities are becoming more and more important. Wireless networks are a little more secure than Bluetooth, but as wireless LAN is generally used in a more critical environment it is more serious. With both Bluetooth and wireless LAN there are ways of protecting communication, but correct implementation requires experience and skill.

6.3.3 Radio Frequency Identification (RFID)

This technology is being used in more and more areas, e.g. Swedish passport documents, stock goods, medical packaging, entry systems and public transport.

During 2008 several research teams recorded discouraging security deficiencies in the Mifare circuit supported by RFID. The circuit is used in a lot of cards and keys worldwide. It transpired that copying of the cards without having physical access to them was possible using wireless readers. Major investment in a new national public-transport ticket system in the Netherlands is being delayed pending resolution of the problem of these weaknesses.

RFID can be used to gather information on a specific product and trace its geographical location. In terms of integrity and societal considerations there are thus many issues to which attention should be drawn. The technology is relatively cheap and there are many applications. As mentioned above, the technology has its shortcomings, and it is extremely important to emphasise the issue of security in this field.

6.3.4 Websites

Vulnerabilities in internet applications are increasingly often being exploited by attackers with various aims, and the attacks have attracted great attention in

[140] PTS-ER- 2007:16 p. 29

recent years. SQL injections began to attract attention at the end of 2007, and during 2008 a large number of attacks of this nature were recorded. SQL injections usually target databases or database servers, and are usually made possible by the web developer's negligence in checking which data the user can send using forms or internet-address fields. The underlying problem is often a lack of processes and control. Many websites start on a small scale and then quickly expand, with the introduction of more users and new functions. As the websites were not designed for such use from the start, safety issues are easily marginalised. In several instances a lack of knowledge about threats, vulnerabilities and the security measures available probably also lies behind these weak spots. No security tests or security analyses are carried out, the emphasis instead being on user-friendliness and functionality.

If there are too few people building and administrating a website in relation to the number of users, e.g. as a result of the site's rapid increase in popularity, security work may be neglected. Aggressors can cause damage using methods of attack such as *Drive-by downloads, Remote file inclusion* and *Cross-site scripting*, e.g. by stealing passwords or changing content. Exploitation of a lack of security on popular websites with many visitors is of particular interest.

It is important for users to be able to rely on internet content and for sensitive information, e.g. passwords, to be protected. In the cases highlighted in 2008 involving theft of user names and passwords, the consequences were exacerbated by the fact that many people used the same password for several different websites.[141] Using a single stolen user name and the relevant password one attacker was able to access several personal websites. There are solutions to counteract this, e.g. OpenID, but people still tend to be dubious about security, and this affects confidence in these solutions.

It is also common for malware to be designed to resemble antivirus programs. The websites with malware are then structured so as to be reminiscent of the antivirus companies' websites. By giving the impression that the programs are security programs it can often be easier for attackers to get victims to install malware themselves than for the attackers to try and exploit the websites' vulnerabilities. In some blogs and social networks insertion of code is permissible. This facilitates dissemination of malicious code such as viruses and trojans to other users, which in turn can decrease confidence in this type of service.

6.3.5 Time

In addition to organisations that provide communication-network and communication services, a number of societally important operations and services are dependent on access to traceable time, including the Swedish

[141] This was the case, for example, with the data incursion into the Swedish Information Processing Society in February 2008, when log-in details of 26,000 members were stolen.

Central Bank (Riksbanken), the Swedish Rail Administration, the RAKEL system, the Swedish Civil Aviation Administration and the Swedish Transport Agency. There are currently several ways of collecting time, e.g. using the Global Positioning System (GPS) and Network Time Protocol (NTP) servers, which are available through the internet and TV.

In a communication society in which hundreds of thousands of systems communicate with each other it is essential that the time scale be unambiguously defined and the degree of correctness and robustness be set. Unless these issues are addressed incident investigations, for example, will need an unreasonable amount of time and will require unreasonable expense for reconstruction of chains of events. One of the most serious deficiencies of unsynchronised systems is that log data can be misleading. This can lead to hacking becoming hard to follow up and bank transactions getting harder to trace.

The situational assessment included a study of how correct and traceable time is used in organisations that carry out societally critical operations. Awareness of the source of time in use varies from organisation to organisation, but those organisations whose activities affect critical societal functions are well aware of it. There is great confidence in GPS-based technology as a source of time. Certain organisations use GPS as the sole source of time, which may be deemed inappropriate, as this source is relatively disturbance-sensitive and is controlled by a state other than Sweden. Vulnerability generally increases when time is only collected from a single source, regardless of whether it be GPS or NTP.

A serious shortcoming of several of the organisations is lack of knowledge of the localisation of the NTP servers used as the primary source of their own time. Awareness of the existence of national NTP servers that guarantee high-quality time data, e.g. at SP Technical Research Institute of Sweden[142], should be greater than is currently the case. An NTP server provided by an unknown operator somewhere on the internet may lack robustness, correctness and availability. It is up to each and every time-server operator to be responsible for these properties, and this can mean that availability and quality may vary. If, however, the societally important activities use several known and stable national sources, it will be increasingly likely that quality – above all amongst collaborating businesses – will be retained or enhanced. More recent versions of the NTP protocol also offer cryptographic functions that could bring the business time data that is far more correct and traceable than that usually used at present.[143]

There is a lack of information on how express policies and guidelines on time are to be handled, but the perception is still that these issues often form part of the organisation's policy/regulatory framework for their other IT security work.

[142] http://www.sp.se/

[143] NTP autokey, for further information see, for example, http://www.ntp.org

Audits of prioritisation in log-data collection and recurrent analyses of how the business can best guarantee its access to time and synchronisation of time between different systems are currently only carried out by the most time-critical organisations. With regard to time, both the dependence on disturbance-sensitive time sources and the lack of signed time sources in the form of signed NTP servers should be taken into consideration by the operators carrying out societally important activities.

6.3.6 Domain Name System (DNS) and Border Gateway Protocol (BGP)

Domain Name System (DNS) is a distributed database that is available using a global hierarchical network of DNS servers. DNS is used to find information on allocated domain names on the internet. It translates IP numbers into domain names and vice versa. The internet is currently dependent on a well-functioning DNS. DNS brings a number of security risks, e.g. it is possible for an attacker to manipulate answers to DNS questions in order to route traffic from a website to his own site.[144] Security can be increased by the website holder using the service DNS Security Extensions (DNSSEC). This means that the website holder allows visitors to check that they have actually reached the right website, using an electronic signature. Using this service you can detect whether the address reference, e.g. to a specific website, has been falsified.

Border Gateway Protocol (BGP) is a routing protocol that holds the internet together. It has proven that BGP features serious security deficiencies, which means that an attacker can monitor unencrypted internet traffic anywhere in the world and modify the traffic before it reaches its destination – all without being detected. A so-called man-in-the-middle attack was demonstrated by two researchers in August 2008. This kind of attack uses BGP to deceive routers into forwarding data to an interceptor's network. The method can be used for company or state espionage, or by intelligence services that wish to intercept or monitor internet data without the collaboration of data and telecom operators.

An event that attracted great attention in 2008 was when Pakistan Telecom wanted to stop users in Pakistan accessing YouTube so as to avoid residents of the country gaining access to content that the Pakistani government deemed unsuitable. By mistake the company incorrectly routed the traffic in the BGP routers. This meant that for two hours many people all over the world could not access YouTube and instead came to a site in Pakistan that was intended for its residents.

[144] This can be with the intention of deceiving visitors into believing that they have got through to their internet bank, whilst they have in fact been redirected to a false site. If the visitor supplies details of user name and password, on the false page this information can under certain conditions be used by the attacker to gain access to the visitor's bank accounts.

6.3.7 Archiving

It is very important that data and information be stored in such a way as to meet the need for confidentiality, integrity and availability. There are several different stipulations governing the nature of archiving. The National Archives of Sweden have for many years been working on the security issues concerning archiving, and at national level the work has been carried out through the Swedish Standards Institute (SIS).

In recent years storage of digital information has increased exponentially. For example, an astonishing 36 times more information was stored digitally in 2007 than in 1998. Storage is swallowing up more and more of organisations' budgets.

With digital archiving, uniform and supplier-independent formats and standards should be selected. There is often no policy on saving of information in digital form. There has instead been consistent investment in more storage space, but if structuring of backup copies has not been well thought-out the information may lose its searchability, thus it will lose much of its value. There are systems for email archiving and document management, but they are often perceived to be complicated and are not utilised by users. It is important for an organisation to draw up a policy on what should be saved, why and for how long, plus the relevant regulatory framework.

Alongside the technical challenges of archiving, deficiencies with regard to legal regulation should also be highlighted. The applicable regulation is described by experts in the field as being hard to access, overlapping, often outdated and poorly adapted to the 'IT era'.[145] Of the two general laws applying to the area – the Swedish Book-Keeping Act[146] and the Swedish Personal Data Act[147] – the latter provokes the most questions. The lack of guidance in the form of legal settlements means that much is still unclear with regard to application.

6.3.8 Outsourcing (external handling of services)

The outsourcing companies are handling more and more of society's information and the concomitant security issues. The advantages mentioned are cost savings and the fact that vulnerability in operations and administration in many instances decreases, as the suppliers' technical capacity and expertise are often greater than those of the purchaser. The disadvantages include weakening of the purchaser's expertise and the creation of dependency between purchaser and supplier, above all in the longer term. The dependency makes it hard to retrieve a business once it has been outsourced. It is also of fundamental importance that the information can be protected. Suppliers must

[145] See, for example, Computer Sweden, *The laws on storage are unreasonable,* 2009 01 30, p. 10 f.

[146] Swedish Book-Keeping Act (1976:125)

[147] Swedish Personal Data Act (1998:204)

be able to ensure continuity both in the customer's business and in their own organisation.

There is great variation in customers' stipulations of requirements regarding security in general and continuity planning in particular. A few customers have well-developed specifications of requirements including comprehensive and detailed requirements, though the level of dissemination is very high and the stipulation of requirements is generally weak. Some customers hardly stipulate any requirements at all, and make do with the basic level provided by the suppliers as standard. The availability requirements are by far the most important for most customers. There are deemed to be two explanations for the weakness of stipulations of requirements:

- Lack of knowledge or naivety. Many customers appear to have limited knowledge of continuity planning, and are unaccustomed to performing risk analyses and risk assessments.
- Cost restraint. Most customers appear prepared to take risks so as to keep costs down.

In many instances customers have blind faith in the security included in the basic service, and thus do not put forward their own additional requirements regarding continuity planning. This can also be because of suppliers' behaviour, partly as they try to sell security above and beyond the basic offering, and partly as they are very keen on emphasising the security already provided in the basic service. This approach can lead to customers not ordering further security.

Procurement within the public sector is legally regulated, and many authorities use price as the sole criterion when evaluating incoming offers. This leads to a dilemma for suppliers when formulating tenders in response to the invitations for tender they have received. They then offer a service package that precisely meets the minimum security requirements stipulated in the tender documentation. Suppliers will do this even if they suspect or are convinced that the customer needs better security. The Swedish Public Procurement Act (LOU)[148] can in some instances be counterproductive with regard to favouring a security-based approach and quality considerations in the authorities.

The main aim of continuity planning is to ensure that a business can also operate in the event of incidents and disturbances. There are major deficiencies with regard to outsourcing in this respect. The continuity plans that nevertheless exist focus too much on technical solutions. The interaction between the supplier and the business is usually deficient or non-existent. It is the contact with this business that determines how smooth and secure the continuity planning will be in the event of a disturbance. But such contact rarely exists, contact with suppliers usually being through the customer's IT staff.

[148] Public Procurement Act (1992:1528)

The general pressure on cost-effectiveness means that plants are becoming bigger and bigger, and no supplier can maintain a level of overcapacity sufficient to allow total takeover of operations from a bigger plant that has been put out of action. In these situations one is forced to prioritise, agreements with customers being the governing factor. Customers who have bought backup capacity in another plant and those with double operations come first.

In conjunction with more extensive disruption of operations or emergencies, e.g. an entire operational facility being put out of action, the suppliers' actions often depend on the situation regarding the customers' mutual handling order, and the prioritisations are not something that the customers are notified of. The existing rules of thumb state that the very most important measure is restoration of internal infrastructure as quickly as possible, as it constitutes the basis of a return to normal operations. Way down in the list of priorities come societally important businesses, unless they have paid for a higher level of service. Most suppliers know their customers and know which businesses are the crucial ones for them. This means that the suppliers prioritise things themselves without any actual contact with their customers.

7 Measures for increased security

7.1 Introduction

A description of the current work on increasing security is crucial to the ability to provide a fair picture of societal information security and analyse developments. Under the heading of 'Measures for increased security' we have gathered a number of examples of various measures that in our opinion promote or have otherwise influenced societal information-security work during 2008 or early 2009.[149] There has been a particular focus on authority initiatives, regulation, standardisation, international initiatives and practice/training. We deem the plans of action and the international initiatives to be of particular importance.

7.2 Authority initiatives

2008 was characterised by relatively extensive activity on the part of the authorities, several actions and measures having a direct bearing on the field of information security. It is of particular interest that the year has seen three plans of action dealing with information security from various standpoints – two completely new ones and one that was updated in early 2009. Continuing development is taking the form of reinforcement of future infrastructure through national and international measures.

7.2.1 Action plan for information security in Sweden

The government has commissioned MSB with administrating the national plan of action for information security drawn up in 2008. The plan is based on the national information-security strategy and was drawn up in collaboration with a number of other authorities and organisations with crucial remits in the field[150]. At the end of the year MSB will list the measures that the authority and other authorities concerned have carried out on the basis of the plan of action.[151]

[149] There is a focus on measures of a more general nature. Alongside this, there may be crucial measures in various fields, e.g. the energy sector. For reasons of space we have chosen not to report on them in this situational assessment.

[150] Work is currently in progress within MSB on submitting proposals for update of the national strategy on the basis of current societal developments. The proposal must be submitted to the government in 2009. See further regarding the strategy in Chap. 2.1

[151] Official document on appropriations for the fiscal year 2009 regarding the Swedish Civil Contingencies Agency (MSB)

The plan of action comprises a total of 47 proposed measures for enhancing societal information security, from both a broader and a narrower standpoint. Four areas have been identified as priorities.

- There is a need for improved *multi-sector* and *inter-sector* work on societal information security. Comprehensive information security regulations could be designed so as to apply to all authorities under government control. Responsibility by sector simultaneously needs clarifying. Opportunities to issue appropriate recommendations to other sections of society are also needed.
- A *basic security level for societal information* security needs to be established. A basic level such as this is a prerequisite for safeguarding the information assets that have increasingly become fundamental to both commerce and the public sector.
- Society must be able to handle extensive IT-related disturbances and crises. An *operational national coordinating function* should thus be established.
- There is a lack of information security expertise at all levels of society. The rapid development also means that lack of skill in individual users is having bigger and bigger consequences. Several proposals are thus being presented that together constitute a wide-ranging investment in *skills enhancement* in the field.

In 2008 work began on a number of measures. This included commencement of the work on supporting the authorities' application of LIS (Management System for Information Security – SS-ISO/IEC 27001 and SS-ISO/IEC 27002) within the project Basic Information Security[152], and the training sector was investigated with the aim of forming a basis for skills-enhancement measures. A further raft of measures is planned for 2009.

The proposals presented in the plan of action are measures in the field of information security, and cover the whole of society from normal conditions through to a crisis situation. They are concrete measures, most of them with the aim of reducing vulnerability in businesses, e.g. by drawing up information and recommendations on how information security should be dealt with in procurements and stipulating that authorities record in their annual report how current information-security requirements are being met. Many of the measures seek to generally increase expertise and awareness of information security, whilst the aim of others is to increase knowledge and collaboration in a specifically identified area, e.g. digital control systems. All of these and other proposed measures basically have a direct affect, in the long or short term, on threats and vulnerabilities/risks emphasised in the situational assessment.

When all 47 proposed measures have been carried out, societal information security will be far better than it is today. The plan of action has broad support from crucial parties in the field of information security, and supports most

[152] See below section 7.2.4

objectives for the information-security work that has been set up in the current strategy for societal security work.

7.2.2 Action plan for e-government

The Swedish Administrative Development Agency VERVA, which ceased to operate at the end of 2008, was commissioned by the government to manage and coordinate public administration's development work on secure exchange of information and secure handling of electronic documents. According to the government's plan of action for e-government[153], electronic identification is an important factor for confidence and dialogue between authorities, residents of Sweden and companies. The reason for this is that in many cases there is a need for secure identification, signature and protection of personal integrity.

Security issues in the public sector have been closely linked to the development of electronic services (e-services) that has been in progress since the mid-1990s. There has always been great pressure to develop secure solutions for electronic identification and signatures. Since the beginning of the 21st century well disseminated solutions for identification and signing have been available electronically through procurements under a general agreement on the part of the Swedish Agency for Public Management and VERVA. A number of banks and TeliaSonera are issuers, and over 1.5 million people in Sweden now use their electronic ID for public and private e-services every month.

Use of the current electronic ID has in many ways been successful, though not yet totally unproblematic. The problems experienced have chiefly involved the provision model and usage. The issuers' concept has entailed certain difficulties because of the technical complexity, and applied price models have been found to be problematic.[154] Some people have found use of electronic ID inflexible. Not everyone who needs electronic ID has been able to get it, e.g. those under the age of 16 and refugees without identity documents or bank balances.[155] Over the years the security of the solutions has also been questioned. Criticism has been levelled at use of so-called soft certificates (certificates and encryption keys stored in a data file), which have not been deemed to meet reasonable security requirements. The security of the 'soft' certificates has gradually been improved by the suppliers, however, and no incidents connected with the vulnerability of 'soft' certificates are known of in this context. But there is a widely held view that development should be towards increased use of smartcards or solutions offering an equivalent security level.

[153] Plan of action for e-Government – New reasons for IT-based business development in public administration, Fi2008/491, Government Decision 17.01.2008

[154] VERVA, *Final report on secure exchange of information and secure handling of electronic documents*, 2008:12

[155] The dismantling of the Swedish cash service has meant that individuals are now obliged to apply for identity documents at banks. Without any credit balance or identity documents, however, electronic ID has proven difficult to obtain.

VERVA's report Electronic identification and signature in Sweden[156] assessed that a general and common infrastructure for electronic ID makes it easier for organisations offering e-services to provide simple, practical solutions. A general solution creates predictability for users. Predictability in turn creates security and confidence. VERVA proposed that the government ensure that there be an electronic-ID system regulated for Sweden that provides support for both qualified and advanced electronic signatures, and the national ID card is to be usable as a bearer of Swedish electronic ID.

7.2.3 Action plan for internet security

PTS is the sector's authority for electronic communications, including the internet. In 2006 the authority was commissioned with presenting a proposed strategy for a more secure internet in Sweden, and it was adopted by the government that same year.

The strategy targets those sections of the infrastructure that are unique to the internet, and as well as strategic considerations it also includes a plan of action for achieving the objectives.[157] The vision is for the internet to be secure and fast and to feature a high level of availability for everyone in Sweden within ten years. The plan of action was updated at the beginning of 2009.

The aim of a strategy for a more secure internet in Sweden is to safeguard critical functions in internet infrastructure which, if not maintained, would create extensive disturbances or interruptions and thus impede or prevent use of the internet by large groups of individual users or societally important companies, authorities and organisations. Large parts of the infrastructure are provided by private operators. The starting point for security in internet infrastructure is thus the providers' responsibility for networks and services based on market requirements. The public undertaking is based on there being requirements that the market cannot meet.

With regard to the internet, in 2006 PTS identified a number of trends and threats. The year's situational assessment shows that most of them still remain, two year on. The strategic stances that the trends and the threats caused in 2006 in conjunction with the 2009 update have consequently only changed marginally. They currently comprise the following:

- Internet physical infrastructure should be protected against accidents, disturbances, interception and manipulation of information during transfer.
- Resistance to disturbances in the domain-name system should be increased.
- Resistance to disturbances in exchange of traffic between Internet operators should be increased.
- Users and purchasers should be trained and kept informed for increased security awareness.

[156] Offprint from VERVA Report 2008:12

[157] Strategy for a More Secure Internet in Sweden PTS-ER-2006:12

- Assumption of responsibility for users' security should increase in internet operators and providers of software and equipment.
- National development of knowledge about internet infrastructure should be promoted, and should take place in a broader context concerning information security.
- Swedish participation in international forums should be intensified, and should take place in collaboration between the private and public sector.
- The ability to handle crises related to internet infrastructure should be developed.

The plan of action comprises a number of measures that seek to meet the strategic stances. In accordance with the updated plan of action PTS intends to do the following over the coming two years:

- Promote use of DNSSEC
- Prepare recommendations on more secure exchange of traffic between internet operators
- Prepare the introduction of IPv6
- Reduce dependence on disturbance-sensitive time sources
- Work on skills enhancement
- Study the occurrence of botnets in Sweden,
- Increase its participation in international organisations and
- Seek inclusion of a more secure internet in European strategy for the information society.

A well-functioning and secure internet is a crucial prerequisite for information management in a number of sectors, thus both the strategy and the plan of action constitute crucial tools for societal information security, not least regarding societally important operations and efficient use of IT.

7.2.4 Fundamental information security

One objective for the plan of action for societal information security is, like the strategy for a more secure Internet, to contribute to the work of achieving a robust information infrastructure in society and a basic level of information security.

Work is currently in progress within MSB and with the support of other authorities and interested parties on creating a number of support documents for application of management systems for information security. As an initial stage with the aim of facilitating internal security work, an information-classification model has been prepared.[158] Another stage is to make available the regulations that VERVA drew up for information security on

[158] The classification model will be published in spring 2009.

MSB's website and to begin internal work on preparing them and replacing them with regulations issued by MSB.

7.2.5 National cooperation function

Experience of the attacks on Estonia in spring 2007 shows that IT-based disturbances and attacks not infrequently spread across organisational boundaries at great speed. Organising for this eventuality, not least regarding distribution of responsibility, is thus of great importance. An important proposed measure in the plan of action is thus to create an operational national coordination function with a decent operational capacity during serious disturbances and crises, using existing resources as a basis. A function such as this would also be able to carry out exercises under normal conditions. Joint exercises mean a learning process for several parties, and may also be of great importance if normal conditions develop into a crisis.

Large-scale cyberattacks usually feature a very rapid course of events, the detection and presentation of which thus impose particular requirements. The counter-measures also start immediately on a broad front, and are then necessarily less well coordinated. The ability to quickly clarify the situation and coordinate the measures to be undertaken is therefore important.

This situational depiction, however, is only part of all the information arising in a specific situation. It is thus important to be able to exchange information between a number of parties involved. It is also important to understand that the time-criticality of items of information in the situational depiction varies depending on the type of attack or event to be handled, but maybe the very most important factor is for the person or persons with the remit and resources for handling the situation to be given all the relevant information.

The aim of setting up an operational national coordination function is for there to be efficient dissemination of information in the field of societal information security as a whole, through which the parties concerned can achieve a combined level of knowledge and situational assessment and attain the operational ability necessary for communication and action in conjunction with incidents and crises. This also means that skilled and practised staff must be available in the event of a crisis.

With regard to MSB's remit, it is natural that the authority has a crucial role in maintaining part of a national situational depiction. Work is currently in progress on creating an administrative and technical infrastructure for issue of information and responses in a broad sense in the field of information security in Swedish society. The bottom line is basing things on and taking into account present activities, e.g. CERT activities at Sweden's IT incident centre SITIC and existing intelligence operations within the police force, the Swedish Security Police, the Swedish Armed Forces and the Swedish National Defence Radio Establishment (FRA).

7.2.6 Swedish Government Secure Intranet (SGSI)

Several of the threats we have listed in Chapter 5 are connected with insecure network environments. SGSI is an encrypted and protected authority network

connected to the EU's secure network S-TESTA, to which only one connection per member state is permitted. Since the network went into operation in 2004 its security has been developed further. This has happened through continuous analysis of the threats and risks occurring, which then form the basis for development of the security process.

The SGSI network was designed to meet stringent availability requirements, and can now offer a far higher level of operational security and availability than the internet. Operation and maintenance are handled by staff from the Swedish National Police Board, the Swedish Armed Forces and TeliaSonera together with the accredited authorities' local technicians. SGSI currently comprises around twenty authorities. All of these authorities meet the security requirements applying to connection to the network. If authorities communicate with each other within the country, connection to SGSI should be considered so as to avoid exposure to the potential risks of unprotected networks. This applies, for example, to future e-government, as residents of Sweden must be able to contact a single authority via the internet and then get a matter resolved in its entirety, even if the authority has to collect part of the information from other authorities.

7.2.7 Cryptographic functions

There are currently nationally approved cryptographic systems for protection of electronic communication in the form of systems for encryption of telephony in fixed and mobile telephone networks, telefax and video conferencing and for protection of data communication and data files. They must facilitate inter-sector coordination between the Swedish Government Offices, authorities and certain companies. The nationally approved systems have been security-checked by the Swedish Armed Forces, who guarantee that there are no implanted or unintentional weaknesses in the cryptographic function. Some systems are also checked by the Defence Matériel Administration (CSEC) in accordance with the Common Criteria standard. There are currently nationally approved encryption systems for protection of information that concerns Swedish security and that is covered by confidentiality in accordance with the Swedish Official Secrets Act[159]. There are also systems that can be used to protect confidential information that does not concern Sweden's security and for other sensitive official information. Most systems can be used both nationally and on international trips, or for exchange of information with staff from other states, the latter requiring government approval and the requisite agreement between the parties.

MSB decides which civil authorities or other organisations are to be allocated nationally approved cryptographic systems. Following consultation with MSB the Swedish National Defence Radio Centre (FRA) is acquiring the cryptographic material required for societal protection and contingency arrangements. FRA then supports the authorities that use nationally approved

[159] Official Secrets Act (1980:100)

cryptographic systems and provides the training required for authorisation in handling of such systems.

At local level there is currently no access to nationally approved cryptographic systems. During 2009 work is being commenced on offering the municipalities nationally approved cryptographic functions within its operations and for secure exchange of information with government authorities.

7.2.8 DNSSEC

Deficiencies in the structure of the domain-name system make it possible to give a false identity so as to provide a specific website. This makes it possible to get users to think they have accessed their bank and then fraudulently obtain log-in details and codes from them.

To protect oneself against this type of attack you can use DNSSEC, i.e. utilise an electronic signature to allow users to securely check that they have really reached the right website. This service allows you to detect whether the address reference, e.g. to a website, has been falsified.

During 2008 interest in the DNSSEC service offered by .SE greatly increased, and by November 1,000 .SE domains had been signed. In order to further highlight the advantages of the technology, PTS was the first government authority to sign its website.

7.3 Regulation

Protection of information is a crucial legal remit, and in recent years a number of measures and initiatives with a bearing on the field of information security have been undertaken. The following review has no ambition to be comprehensive, but focuses on regulatory measures deemed important for societal information security. This year the legislator has paid particular attention to authorities' and other organisations' information management, the work of combating crime and terrorism and protection of personal integrity in the field of medical care and healthcare.

7.3.1 A more secure information handling environment

On 1 January 2008 *VERVA's Regulations for the application of information security standards by government agencies* came into force.[160] According to Section 2 the aim of the regulations is for the authorities to create conditions for secure and reliable exchange of electronic information by applying to their activities the security necessary for their individual requirements. The regulations are crucial to the authorities' information security in that they stipulate requirements for methodical work on information security. Every authority must apply a management system for information security, and bearing in mind risk and vulnerability analyses must decide which risks are to be eliminated, reduced or accepted. The regulations are an important link

[160] VERVAFS 2007:2

between a regulatory approach and standardisation, as they expressly stipulate requirements for the form of the work to be in accordance with the information security standard ISO/IEC 27000. At the end of 2008 VERVA ceased to operate. The regulations are still in force, and an investigation carried out by VERVA shows that the majority of the authorities investigated have introduced the regulations or started to follow them.[161]

As there is a need for clear regulatory frameworks and guidelines in the field of information security, MSB was authorised in the *Ordinance on Emergency Preparedness and Heightened State of Alert (*2006:942)[162] to announce regulations on information security, taking into consideration national and international standards. The work on the regulations is in progress within the authority, and when it is finished they will replace VERVA's regulations on information security.

An important prerequisite for attainment of the desired level of information security is order and control of information management. An important part of this work is clearly identified responsibility. In a number of reports issued between 2005 and 2007[163] the Swedish National Audit Office pointed out deficiencies regarding authorities' internal management and control of information security. This applied not least to management's understanding and its work on managing and assuming responsibility for the work on information security. Since 1 January 2008 management's responsibility has been clarified in an *official ordinance*.[164] *The Ordinance on Internal Management and Control*[165] clarifies management's remit and stipulates requirements regarding risk analysis, control measures, follow-up and documentation.[166]

All the above regulatory frameworks contribute to efficient and secure information management in authorities, but it is important to make sure that the work on the regulatory frameworks be coordinated, e.g. with regard to the requirement for risk analyses.

Information management in big companies has increasingly become regulated. The bottom line in this context has been to impede financial crime, identify responsibility and increase public control. A fundamental regulatory

---

[161] VERVA, *69 authorities describe 915 strategic measures for development of e-government,* 2008:14, p. 24

[162] Sections 30a and 34 Ordinance (2006:942) on Emergency Preparedness and Heightened State of Alert

[163] See, for example, RiR 2005:26 Audit of Swedish National Government Employees Salaries and Pension Board's Internal Management and Control of Information Security and RiR 2006:24 Audit of the Swedish National Labour Market Administration's Internal Management and Control of Information Security

[164] Official ordinance (2007:603)

[165] Ordinance (2007:603) on Internal Management and Control

[166] The Swedish National Financial Management Agency can announce the regulations required for realisation of the ordinance.

framework is the American act *Sarbanes-Oxley, SoX*.[167] Within the EU equivalent work has chiefly taken place through the *4th, 7th and 8th company-law directives*[168]. The latter has brought about changes in the *Swedish Code for Corporate Governance*[169], and the changes came into force on 1 July 2008.

An investigation that may gain great significance for security and information management is The Legal Position on Backup Copies (Swedish Government Official Report SOU 2009:5). The investigation proposes that backup copies should be exempted from the constitutional regulations regarding general documents[170].

7.3.2 Crime prevention and fighting crime

With regard to the possibility of gathering information in order to prevent and fight crime, a number of changes were carried out or investigated in 2008. One of the laws most written about and debated is the *Act on Signals Intelligence in Defence Operations*[171], which came into force on 1 January 2009. On certain conditions the law allows the Swedish National Defence Radio Centre (FRA) surveillance using cable, thereby expanding on the previous restriction to surveillance over the Ethernet. According to Section 1 of the law FRA can gather signals in electronic form for intelligence operations within the parameters of the arrangements stipulated by the government or by the authorities stipulated by the government. Examples of such authorities are the Swedish Security Service (SÄPO), the National Swedish Criminal Investigation Department and MSB. The debate regarding the law chiefly concerned integrity issues, and led to the government presenting a proposal for a change in the law whereby signals surveillance can only be set up by the government, the Swedish Government Offices and the Swedish Armed Forces, the requirement for permits is being tightened up, intercepted information that is particularly integrity-sensitive must be destroyed, and individual access to effective right of appeal is being improved.[172]

A number of commentators predict that the integrity debate will again intensify in conjunction with implementation of the directive on storage of traffic data

---

[167] Sarbanes-Oxley Act of 2002

[168] The Council's fourth Directive 78/660/EEC of 25 July 1978 on the Annual Accounts of Certain Types of Company, the Council's seventh Directive 83/349/EEC of 13 June 1983 on Consolidated Accounts, the Council's eighth Directive 84/253/EEC of 10 April 1984 on Approval of Persons Responsible for Carrying out the Statutory Audits Accounting Documents. The eighth company-law Directive is replaced by Directive 2006/43/EC of the European Parliament and the Council of 26 April 2006 on Statutory Audits of Annual Accounts and Consolidated Accounts and on Amendment of the Council's Directives 78/660/EEC and 83/349/EEC and on Repealing the Council's Directive 84/253/EEC

[169] http://www.bolagsstyrning.se/files/docs/Svenskkodforbolagsstyrning.pdf

[170] Freedom of the Press Act (1949:105) Chap. 2 Section 3

[171] In the media it has often been called the 'FRA Act'

[172] Ministry Publications Series 2009:1 Enhanced Protection of Integrity in Signals Surveillance

for crime-fighting[173] in Swedish legislation. The law requires tele-operators to store traffic data for a year. The aim is to facilitate access to electronic evidence.

The integrity debate has also been updated with regard to the changes in the copyright law that came into force on 1 April 2009.[174] Under certain circumstances it gives copyright holders such as recording companies, publishers and film companies the right to obtain information on IP addresses of tele-operators through the courts. A criticism that has been levelled at the regulatory change is that it gives copyright holders a greater chance of obtaining this type of information from the tele-operators than the police, who are currently restricted by the ruling in the Swedish Electronic Communications Act[175] that the crime in question must be one for which a minimum sentence of six months' imprisonment is prescribed.[176] The limitations on police powers to gain access to this type of information have been the subject of an investigation.[177] A debate has also commenced regarding the so-called IPRED2 Directive and the Anti-Counterfeiting Trade Agreement (ACTA).[178]

7.3.3 Protection of personal integrity

Last year changes in the Personal Data Act[179] attracted great attention in media. This year the new Patient Data Act[180], which came into force on 29 May 2008, is of particular interest. The law supplements the Personal Data Act, and

[173] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[174] See Government Bill 2008/09:67 and Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights.

[175] Chap. 6 Section 22 First Para 3 Swedish Electronic Communications Act (2003:389)

[176] In accordance with Chap. 7 Section 53 Act (1960:729) on Copyright in Literary and Artistic Works anyone making themselves guilty of breach of copyright, if this takes place intentionally or through gross negligence, will be sentenced to a fine or imprisonment for a maximum of two years.

[177] Swedish Official Government Report SOU 2009:1 A more legally secure way of obtaining electronic communication in crime-fighting (Investigation of Police Methods)

[178] IPRED2 Directive: Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (COM/2006/0168 final - COD 2005/0127) and the international agreement Anti-Counterfeiting Trade Agreement (ACTA), which with the aim of combating incursion of intellectual property rights can increase the chances of obtaining information from network operators and can give the right to increased control in the event of border-crossing of portable media such as computers.

[179] Swedish Personal Data Act (1998:204). The amendments mean that the Act as a whole moved from stating what is permissible to instead stating what constitutes abuse (action model to an abuse model).

[180] Patient Data Act (2008:355)

clarifies what applies regarding handling of personal data in the field of medical care and health care. The main aim is to reinforce protection of integrity. Regulation will facilitate both increased patient safety and a high level of protection of integrity. The new law allows a coherent case-record system, which means that healthcare providers can build systems whereby various healthcare providers can gain access to patient information, regardless of where the patient in question is seeking care. Patients are also given more chance to exert influence, e.g. by being able to stop other units within the same healthcare provider and other healthcare providers gaining electronic access to their records. Patients can also gain increased access to log data. The National Swedish Board of Health and Welfare has the right to announce more detailed regulations on security measures concerning handling and storage of case records.

7.4 Standardisation

Alongside regulation, standardisation is a powerful means of control with regard to security work. Many standards have a bearing on the field of information security, but we have chosen to illustrate developments regarding three crucial standards. Particularly with regard to the first two, Sweden has been an active participant in the international standardisation work.

Most organised standardisation work takes place within three different organisations: ISO, IEC and ITU. ISO and IEC collaborate on IT. Standards developed jointly are always given the designation ISO/IEC plus a number. In order to handle joint development, ISO and IEC have formed Joint Technical Committee 1 (JTC 1). Subcommittees responsible for various areas are then organised under the auspices of this committee. SC 27 bears responsibility for all development of standards in the field of information security.[181]

Standardisation operations in the field of information security are characterised by a high level of activity involving a large number of standards that are in the process of development. Sweden has for many years actively taken part in the work within SC 27. Standardisation operations within SIS concerning information security are now gathered in one committee: TK 318.

Internationally within JTC1/SC 27 a total of about 80 standards have been issued or are in the process of development in the area.

Not all standardisation work of interest in the field of information security, however, takes place within ISO and IEC. There are a large number of industry standards and de facto standards that are also important.[182]

[181] There are principally five different working groups working on standards.

[182] For example, the PCI DSS industry standard described below for card handling and the Windows operating system's dominant position on the market.

7.4.1 ISO/IEC 27000 Information security management systems (LIS)

The series of standards SS-ISO/IEC 27000 Information Security Management Systems is crucial to the field of information security. It sets a framework for and supports an organisation's development of policy and objectives and its work on achieving its objectives. The SS-ISO/IEC 27000 series now forms a natural focal point for all standardisation in the field of information security, and in areas where other standards seek to relate to the above series. It can simultaneously be stated that the SS-ISO/IEC 27000 series is having an increasing impact both internationally and within Sweden.

During 2008 the 27000 series was expanded to include a standard for risk management in the field of information security, SS-ISO/IEC 27005. Work has also started on revision of the original standards SS-ISO/IEC 27001 and SS-ISO/IEC 27002, which include express requirements and recommendations regarding implementation of requirements. Further expansion of the 27000 series is planned for 2009, when ISO/IEC 27003 concerning Introduction of Information Security Management Systems and ISO/IEC 27004 concerning Information Security Measurements will be completed and issued.

During 2009 an overall standard involving terminology and an overview of the 27000 series will also be issued. This will be called SS-ISO/IEC 27000, and will be historic in that it will be the first ISO standard ever to be freely published.[183] SS-ISO/IEC 27000 will include definitions and descriptions of the process in LIS, and will constitute a description of both the 27000 series and the 27030 series[184].

Standardisation is assuming an increasingly major role within Swedish public administration. The merger of KBM, the National Swedish Rescue Services Agency (SRV) and the National Board of Psychological Defence (SPF) means that the new Swedish Civil Contingencies Agency (MSB) is assuming a more and more important and increasingly clear role as the authority with responsibility for coordination in the field of information security. The Ordinance on Emergency Preparedness and Heightened State of Alert[185] emphasises that the regulatory responsibility that accompanies the new authority's responsibility must be based on standards in the area. VERVA's regulation in this field already emphasises that government authorities must introduce a management system for information security (LIS), in accordance with SS-ISO/IEC 27001 and SS-ISO/IEC 27002. To facilitate this work MSB

[183] The cost of standards varies. The acquisition cost of a package including ISO/IEC 27001 and ISO/IEC 27002 is usually about SEK 3,000.

[184] The latter includes the multiparty standard Network Security, which is being audited. Other standards concerning continuity planning, incident management, collection of evidence and cybersecurity can also be found in the ISO/IEC 27030 family.

[185] Section 34 Ordinance (2006:942) on Emergency Preparedness and Heightened State of Alert

has bought up and will distribute the above-mentioned standards to authorities covered by VERVA's regulation within this field (government authorities).

7.4.2 Common Criteria

Common Criteria (CC) is a standard for stipulating requirements, declaring and evaluating security in IT products and systems in their application environments. CC is a framework for description of the functional requirements for IT security in a product or system, not a collection of requirements per se. This framework first clarifies the requirements situation so that the product or system can then be evaluated in relation to this. CC focuses on the need for information security (confidentiality, reliability and availability) arising as a result of intentional or unintentional threats.

As part of the Common Criteria Recognition Arrangement (CCRA) international collaboration is in progress for development of the CC standard[186]. There are currently 25 participating countries, the most recent addition being Pakistan, which was accepted as a member in 2008. The standard is an important tool in the work on secure products. In Sweden two products have been certified to date and four are being evaluated. This is to be compared with the situation in the USA, where highly target-oriented work is in progress on only using CC-certified products in government authorities that handle sensitive material.[187]

7.4.3 Payment Card Industry Standard Data Security Standard (PCI DSS)

Stolen card data and card fraud have been a problem in many parts of the world and a concern for the card industry. This year's situational assessment also indicates that illegal handling of personal data is increasing rather than decreasing.

With the aim of making handling of card information more secure and minimising the risk of card-data theft, the international card networks MasterCard and Visa have drawn up the standard PCI DSS, which was originally launched in 2004 but was updated in 2008 to Version 1.2. One aim of the standard is to maintain and reinforce confidence in cards as a method of payment.

All sales companies, redemption agents and third parties that handle, store and/or transfer card information must meet the PCI DSS requirements. The security requirements vary slightly depending on the company's volumes (card transactions), the industry and the risk classification, but include requirements for firewalls, handling of passwords, physical security, logging and security

[186] http://www.commoncriteriaportal.org

[187] The relevant regulatory frameworks in this context are FISMA, Federal Information Security Management Act and Policy 11 (National Information Assurance Acquisition Policy (NSTISSP 11)) For further information see https://buildsecurityin.us-cert.gov/swa/acqart.html

policy. Sales companies or redemption agents that do not meet the requirements risk financial losses and ultimately loss of the right to receive cards as a method of payment.

It is deemed that the standard and its concomitant security requirements will in general increase security in the parties concerned and will in the long term increase customer confidence in the card-payment system.

7.5 International initiatives

Within the work on information security a number of measures are in progress at international level – some of a technical nature and others with a more administrative focus. Well-functioning information management is of fundamental importance to one's own society's functions, whilst at the same time the infrastructure utilised by information management, e.g. the internet, is international. International cooperation is in this context vital to attainment of sufficient security. In the situational assessment we have chosen in particular to illustrate some of the measures undertaken within the EU and the UN. In addition to activities within these organisations important work is taking place in a number of international organisations such as ICANN and IETF, in particular with regard to the internet.

7.5.1 ENISA

ENISA[188] is an EU authority with the remit of supporting member states, EU bodies and companies in their work of maintaining a high and efficient level with regard to information security. ENISA also acts as a centre of expertise for the member states and the EU institutions, facilitating exchange of information and collaboration. The organisation gathers and analyses data on security incidents and risks, and is doing active work on awareness-raising measures.

The objectives for 2009 are:

- To improve robustness and capacity for recovery in European electronic communication networks
- To develop and maintain the collaboration between member states
- To identify new risks in the field of new technology and services

7.5.2 Organisation for economic co-operation and development (OECD)

The OECD has for several years devoted itself to the issue of information security. A fundamental document in this context is the organisation's *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* dating from 2002.[189] At its meeting of ministers in June

[188] See http://www.enisa.europa.eu

[189] See http://www.oecd.org/dataoecd/42/57/32494705.PDF

2008 the organisation focused on RFID[190] and digital material[191]. The organisation has also issued recommendations for Protection of Critical Information Infrastructures.[192]

7.5.3 Internet Governance Forum (IGF)

The IGF seeks to support the UN Secretary-General in realising the remit of the World Summit on the Information Society (WSIS) of creating a new forum for policy discussions for all the relevant parties with regard to control and development of the internet. Work on promoting security and confidence were high up on the agenda at the most recent meeting in December 2008. Unlike at meetings in previous years, a whole day was devoted to the issue. At the meeting it was stated that security was the key to creation of confidence in e-trade, e-administration and other online activities, and that security may be the toughest challenge for everyone involved. The importance of collaboration between a number of different parties so as to facilitate handling of threats such as viruses, phishing, espionage and botnets was emphasised. According to the IGF an important prerequisite for such collaboration is creation of confidence between those involved.

As the internet, and consequently all security issues connected with internet use, are of international interest, it is important that the IGF clearly emphasise the need for international measures and cooperation, and offer a platform for such work.

7.5.4 European Program for Critical Infrastructure Protection (EPCIP)

The Directorate-General for Justice, Freedom and Security is financing a study that illustrates the dependence of ICT (Information and Communication Technology) on energy, finance and the transport sector. The aim of the study is to create better understanding of the threat to critical infrastructure and the security risks that should be dealt with. The study will also examine the possible consequences at societal level. The objective of the study is to indicate:

- Methods of assessing critical infrastructure's dependence on ICT
- Agreement on and definitions of what is deemed critical
- Guidelines on reducing the IT threat to critical infrastructure
- Recommendations on security measures that might form the basis of decisions, both for owners of critical infrastructure and for decision-makers at EU level

---

[190] Three Reports from the OECD on RFID have been collected in one document: OECD Policy Guidance on Radio Frequency Identification, Radio-Frequency Identification: A Focus on Security and Privacy and RFID Applications, Impacts and Country Initiatives 2008 http://www.oecd.org/dataoecd/19/42/40892347.pdf

[191] OECD, *Policy Guidance for Digital Content*, 2008

http://www.oecd.org/dataoecd/20/54/40895797.pdf

[192] OECD, OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35] see http://www.oecd.org/dataoecd/1/13/40825404.pdf

The study was initiated at the beginning of September 2008 and is being carried out in project form. The project is to deliver its report at the end of July 2009. As a natural part of this work the project group will work closely with the Commission, owners of critical infrastructure, authorities, organisations and research bodies.[193]

7.5.5 International cooperation

Development in the field of cybersecurity has led to a need for international cooperation. In cooperation with other countries several national initiatives have been undertaken to reinforce national security in the face of cyberthreats. The American Cyber Security Initiative, which was initiated in 2008, is an example of a very extensive initiative.

Nearly a year after the large-scale network attacks on Estonia the NATO defence ministers agreed on a cyberdefence policy, which was adopted at the beginning of 2008. The policy includes development of a response mechanism in the event of a cyberattack.[194] NATO has also developed a concept for cybersecurity issues.[195] The member countries are being encouraged to reinforce their key infrastructures, share experiences and knowledge – so-called best practice – and ensure they can provide support if any of the member countries requests assistance in the event of an attack.[196] Internal collaboration in the event of an attack, e.g. personal networks of (political) leaders and experts, cooperation between the private and public sector and preventive defence, is also being emphasised.[197] In April 2008 a decision was furthermore made on setting up a new centre of excellence for cybersecurity in Estonia, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), which has now commenced its operations.[198]

NATO's previous stipulation was that one should only use the organisation's resources to protect one's own networks. The policy that has now been developed also includes the member countries, and during the attacks in Georgia in 2008 NATO sent out staff to provide support – something that possibly indicates an even broader area of cover, bearing in mind the fact that Georgia is not a NATO member. Within the EU work is also in progress on a review of the field of cybersecurity, and discussions are in progress on how to relate to it.

7.6 Exercises and training

IT is now being used throughout society – and by nearly every resident of Sweden. This means it is vital for individuals to have knowledge of information

[193] http://ec.Europe.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm

[194] Nina Wilhelmson Swedish National Defence College (FHS)

[195] http://www.NATO.int/docu/update/2008/05-may/e0514a.html

[196] Bucharest Summit Declaration (art. 47)

[197] Nina Wilhelmsson, Swedish National Defence College (FHS)

[198] http://www.ccdcoe.org/

security so as to be able to protect their information and the transactions they carry out. In addition there is the consideration that by virtue of their actions everyone contributes to society's joint security and robustness.

It is important that training in information security reach all groups of society. The residents of Sweden must therefore be taught at an early stage to understand the risks of handling IT and the internet. This understanding must constitute an integrated and natural part of schooling, and must be included in higher education.

Training in and understanding of information security are crucial to the ability to achieve the objectives in the field of information security. We have thus chosen to describe two new training ventures and two major exercises that have been implemented.

7.6.1 Chief Information Assurance Officer (CIAO)

In collaboration with MSB, the Swedish National Defence College has started a quality-assured CIAO course. The course, which has been established for a long time and is implemented at the American National Defense University (NDU) and their Information Resources Management College (IRMC), has now been modified for a Swedish/European target group. The aim of the CIAO course is to focus on information and increase the capacity for balanced risk management involving staff, processes and technology in order to achieve the business's objectives. It is chiefly aimed at those with a crucial role in businesses' work on information security.

7.6.2 SIS Information Security Academy

During 2008 SIS launched its Information Security Academy, which is aimed at those who have responsibility for, influence or contribute towards a business's information security. The course structure is in line with the 27000 suite of standards.

With regard to emphasising the standards in the 27000 series in more and more contexts, not least in legal regulatory frameworks, it is important that there be training opportunities.

7.6.3 SAMÖ 08 coordination exercise 2008

An important part of the skills-enhancement work is exercises. This particularly applies to situations in which several different organisations have to coordinate and collaborate on a joint issue.

On 22-24 April 2008 3,000 participants from the Swedish Government Offices, central authorities, county administrative boards, municipalities, organisations, companies and a large public network implemented the cooperative exercise SAMÖ 2008. KBM was responsible for planning, implementing and evaluating the exercise.

The exercise's scenario was extensive logical IT attacks on the financial system. The attacks affected the financial sector, including authorities in the collaborative field of financial security, the police, and parties with geographical area responsibility at national and regional level. Events with

serious consequences for several societally important functions required coordinated measures.

The key word for the exercise was confidence, and its aim was for all parties to be able to say afterwards that through cooperation they had developed their ability to remain confident in societal institutions in a crisis.

The exercise had two subsidiary aims in addition to the main aim: for the parties to coordinate their decisions and measures and thus create a joint impression of the situation, and for the information the participants conveyed to the media and the general public to be credible, relevant and easily accessible.

The evaluators of SAMÖ[199] drew three conclusions:

- The parties did not prioritise cooperation or coordination outside existing networks.
- The parties had insufficient knowledge of other parties' responsibilities and mandates.
- A joint impression of the situation was never created.

Three development requirements became apparent on the basis of these conclusions:

- Improved cooperation in a crisis is most easily achieved through clarification of roles and responsibility. Each party must understand how other parties are affected by individual decisions and measures and have better knowledge of other parties' mandates and responsibilities in a crisis
- Relevant interfaces must be created in everyday life
- Procedures and methods of creating a joint impression of the situation must be clarified.

To sum up, it can be said that the most important focuses for MSB are:

- Intensification of the discussion regarding the situational depiction and the impression of the situation.
- Clarification of report procedures and how information is fed back to the parties concerned.
- Contribution towards increased knowledge of parties' different roles and mandates through exercise and training.

7.6.4 Swedish National Defence College exercise

After the 2007 cyberattacks on Estonia cooperation between Sweden and Estonia started, the aims being to follow developments in Estonia, maintain

[199] KBM, *Evaluation of Coordination exercise 2008*

contacts with SIVAK and create a network for exchange of research. This exchange has resulted in an exercise that took place on 6 December 2008. The exercise was sponsored by KBM, was implemented under the auspices of the Swedish National defence College together with experts from Estonia, and was supported by the Swedish Defence Research Agency (FOI), FMV and FRA. It chiefly comprised intrusion attacks, and the defending teams mainly consisted of Master's students from Linköping University and from Tallinn University of Technology's information security programme.

A number of possible improvements were identified, and continuation at a slightly higher level is planned for 2009, the aim being to make Sweden into a skilled partner and equip it for the international exercise Cyberstorm III in autumn 2010.

Sources and further reading

Public publications

Gov. Bill 2005/06:133 Cooperation in crisis - for a more secure society
http://www.regeringen.se/download/49d6475a.pdf?major=1&minor=60468&cn=attachmentPublDuplicator_0_attachment

Gov. Bill 2001/02:158 Society's security and preparedness
http://www.regeringen.se/download/03c0eac6.pdf?major=1&minor=3260&cn=attachmentPublDuplicator_0_attachment

Gov. Bill 2008/09:67 Civil-rights sanctions in the field of intellectual property rights – implementation of Directive 2004/48/EC
http://www.regeringen.se/download/c18e5f5a.pdf?major=1&minor=116938&cn=attachmentPublDuplicator_0_attachment

Gov. Communication 2005/06:139 National IT strategy for nursing and healthcare
http://www.regeringen.se/content/1/c6/06/03/73/9959f31e.pdf

Plan of action for e-Government (2008)
http://www.regeringen.se/content/1/c6/07/49/95/2c28b30b.pdf

The government's strategy for increased security in internet infrastructure N2006/5335/ITFoU
http://www.regeringen.se/content/1/c6/01/83/13/1c50c06e.pdf

Swedish Official Government Report SOU 2004:32 Information security in Sweden and internationally – an overview (Sub-report from the information-security investigation)
http://www.regeringen.se/download/24f80e10.pdf?major=1&minor=23350&cn=attachmentPublDuplicator_0_attachment

Swedish Official Government Report SOU 2005:42 Secure information
http://www.regeringen.se/download/84506b80.pdf?major=1&minor=44381&cn=attachmentPublDuplicator_0_attachment

Swedish Official Government Report SOU 2007:39 The police of the future
http://www.regeringen.se/download/85343fad.pdf?major=1&minor=83590&cn=attachmentPublDuplicator_0_attachment

Swedish Official Government Report SOU 2007:76 Storage of traffic data to combat crime
http://www.regeringen.se/download/2f8c7424.pdf?major=1&minor=91521&cn=attachmentPublDuplicator_0_attachment

Swedish Official Government Report SOU 2009:1 A legally more secure way of obtaining electronic communications in crime-fighting
http://www.regeringen.se/download/bca06dc6.pdf?major=1&minor=119163&cn=attachmentPublDuplicator_0_attachment

Swedish Official Government Report SOU 2009:5 The legal status of backup copies
http://www.regeringen.se/download/f72be402.pdf?major=1&minor=119810&cn=attachmentPublDuplicator_0_attachment

Swedish Administrative Development Agency (VERVA), VERVA's regulation of government agencies'
work on secure electronic exchange of information, VERVAFS 2007:2
http://www.regeringen.se/content/1/c6/11/82/47/da357c5e.pdf

Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights
http://eur-lex.0europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:SV:PDF

Directive 2006/24/EC of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:SV:HTML

European Commission COM(2007) 267 Communication from the Commission to the European Parliament, the Council and the European Union's Regional Committee: Towards a general policy on the fight against cyber crime
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:SV:HTML

Council of Europe, Convention on Cybercrime CETS No.: 185, 2001
http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Government Reports

Swedish National Courts Administration (Domstolsverket), Specialisation – a preliminary study in collaboration with the Swedish Association of Judges, Domstolsverket Report 2003:3
http://www.dom.se/Publikationer/Rapporter/DV-rapport_2003_3.pdf

Swedish Financial Supervisory Authority, Responsibility for the payment system (2008:10)
http://www.fi.se/upload/20_Publicerat/30_Rapporter/2008/Rapport2008_10.pdf

Swedish Emergency Management Agency, Will we cope with the crisis? Society's capacity to deal with an emergency 2007, KBM's educational series 2008:2
http://www.krisberedskapsmyndigheten.se/upload/17065/klarar vi krisen_temaserien2008-2.pdf

Swedish Emergency Management Agency, Society's information security, Plan of action 2008, 2008
http://www.krisberedskapsmyndigheten.se/upload/17005/handlingsplan samhallets_informationssakerhet_20080401.pdf

Swedish Emergency Management Agency, *Critical societal functions - Suggested definitions of essential functions from an emergency management perspective*
http://www.krisberedskapsmyndigheten.se/upload/16351/Critical%20Societal%20Funktions.pdf

Swedish Emergency Management Agency, Guidance on increased security in digital control systems in critical infrastructure, 2008
http://www.krisberedskapsmyndigheten.se/upload/17913/SCADA_sv_2008.pdf

National Post and Telecom Agency, Botnet-hijacked computers in Sweden, PTS-ER-2009:11
http://www.pts.se/upload/Rapporter/Internet/2009/botnat-i-sverige-2009-11.pdf

National Post and Telecom Agency, Good functionality and technical security in electronic communications, PTS-ER-2008:13
http://www.pts.se/upload/Rapporter/Internet/2008/Tillsyn-god-funktion-och-teknisk-sakerhet-PTS-ER-2008-13.pdf

National Post and Telecom Agency, Strategy for a more secure internet in Sweden, PTS-ER-2006:12
http://www.pts.se/upload/Documents/SE/strategi_sakrare_internet_2006_12.pdf

National Post and Telecom Agency, Security in local wireless networks, PTS-ER-2007:16
http://www.pts.se/upload/Documents/SE/Sakerhet_lokala_tradlosa_nat.pdf

Swedish National Audit Office, Audit of the Swedish National Labour Market Administration's internal Management and Control of Information Security, RiR 2006:24
http://www.riksrevisionen.se/templib/pages/OpenDocument____556.aspx?documentid=6442

Swedish National Audit Office, Audit of Swedish National Government Employees Salaries and Pension Board's internal management and control of information security, RiR 2005:26
http://www.riksrevisionen.se/templib/pages/OpenDocument____556.aspx?documentid=5948

Swedish National Audit Office, Emergency preparedness/ the payment system, RiR 2007:28
http://www.riksrevisionen.se/templib/pages/OpenDocument____556.aspx?documentid=6787

Swedish National Board of Psychological Defence, Analysis of risk and vulnerability in the media sector 2008

Swedish Administrative Development Agency, Final report on secure electronic exchange of information and secure handling of electronic documents, 2008:12

Swedish Administrative Development Agency, 69 authorities describe 915 strategic measures for development of e-government, 2008:14

Miscellaneous

Swedish National Council for Crime Prevention/ Swedish Emergency Management Agency, Cybercrime and incidents – a threat to critical infrastructure?, 2008

CERT-FI, Information security review, 2008
https://www.cert.fi/en/reports.html

Codenomicon white paper, Wireless security: Past, present and future, 2008
http://www.codenomicon.com/resources/whitepapers/Codenomicon_Wireless_WP_v1_0.pdf

Cyveillance, white paper, Online financial fraud and identity theft report, 2008
http://www.cyveillance.com/web/knowcenter/white-papers.asp

Deloitte, Treading Water, the 2007 technology, media & telecommunications security survey, 2007
http://www.deloitte.com/dtt/cda/doc/content/se_treading_water_120208.pdf

Department for business enterprise & regulatory reform (BERR), 2008 information security breaches survey – executive summary, 2008
http://www.berr.gov.uk/files/file45713.pdf

European Network and Information Security Agency, ENISA Position paper, Security issues in the context of authentication using mobile devices (Mobile eID), 2008
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf

Swedish National Defence College CATS, Nina Wilhelmsson, International-law aspects of cyberthreats and protection against information operations, a study based on experiences of the cyberattacks on Estonia 2007, 2008

Georgia Tech Information Security Center, Emerging Cyber Threats Report for 2009, 2008
http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

Google, 2008 annual Google communications intelligence report a Google white paper February 2008, 2008
http://www.google.com/a/help/intl/en/security/pdf/cir_08.pdf

Halon, Q4 2008 Internet Threats Trend Report, 2009
http://www.halonsecurity.ch/press/documents/2008_q4_email_threats_trend_report.pdf

McAfee, Virtual criminology report-Cybercrime versus cyberlaw, 2008
http://resources.mcafee.com/content/NAMcafeeCriminologyReport

Microsoft, Security Intelligence Report, January through June 2008, 2008
http://download.microsoft.com/download/b/2/9/b20bee13-ceca-48f0-b4ad53cf85f325e8/Microsoft Security Intelligence Report v5.pdf

Nohlberg, Marcus, Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks, Stockholm University, 2009

OECD, OECD Policy Guidance for digital content, 2008
http://www.oecd.org/dataoecd/20/54/40895797.pdf

OECD, OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35], 2008
http://www.oecd.org/dataoecd/1/13/40825404.pdf

OECD, RFID Radio Frequency Identification: OECD Policy Guidance - A Focus on Information Security and Privacy - Applications, Impacts and Country Initiatives, 2008
http://www.oecd.org/dataoecd/19/42/40892347.pdf

Reporting and Analysis Centre for Information Assurance MELANI, Information assurance – Situation in Switzerland and internationally, 2008
http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=en

SECODE, Security threats and trends December 2008, 2008
http://www.secode.se/be/__xs_attachments/Threats_and_Trends_December_2008.pdf

SECODE, Security threats and trends February 2008, 2008
http://www.secode.se/be/__xs_attachments/2008-02%20-%20IDS%20-%20Trusler%20og%20Trender-ENG.pdf

Sofaer, Abraham D. & Goodman, Seymor E. et al., A proposal for International Convention on Cyber Crime and Terrorism, CISAC Report, 2000
http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm

Srejber, Eva, Swedish Central Bank, Vulnerabilities in the modern payment system, statement on Swedish Security Assembly in Eskilstuna 18.10.2006

Symantec, Symantec global Internet security threat report, trends for July- December 07, 2008
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

United States government accountability office (GAO), Information security – Although progress reported, federal agencies need to resolve significant deficiencies, GAO-08-496T, 2008
http://www.gao.gov/new.items/d08496t.pdf

Verizon business, 2008 data breach investigations report, 2008
http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Åhlfeldt, Rose-Mharie, Information Security in Distributed Healthcare, Exploring the Needs for Achieving Patient Safety and Patient Privacy, Stockholm University, 2008

MSB Swedish Civil Contingencies Agency
SE-651 81 Karlstad Tel +46 (0)771 240 240 www.msbmyndigheten.se
Publ.nr MSB 0119-09 ISBN 978-91-7383-053-9