

Reflections on civil protection and emergency preparedness during major IT incidents

A study of societal impact following the disruption at Tieto in November 2011

MSB Contact:
Information Assurance Section
Richard Oehme, +46(0)771-240 240

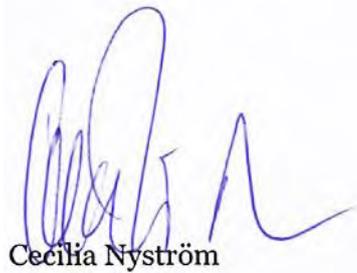
Publication Number MSB 435-12
ISBN 978-91-7383-257-1

Preface

The increased concentration of IT operations and other IT related services, such as cloud services, creates both new opportunities and new risks.

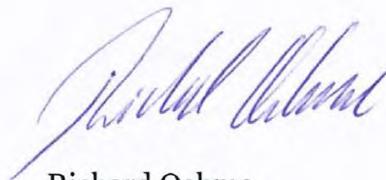
This report is intended to illustrate the societal consequences that may result from a major IT incident based on the disruption at Tieto in November, 2011. In addition, we will study the case from an emergency management perspective in order to learn from the incident.

Stockholm 21/02/2012



Cecilia Nyström

Head, Risk & Vulnerability
Reduction Department



Richard Oehme

Head, Information
Assurance Section

Table of Contents

1. Introduction	9
2. Background	11
2.1 Increased concentration of IT operations and IT related services	11
2.2 Sweden's emergency management system	12
3. Course of events and societal impact.....	15
3.1 General description.....	15
3.2 The technical malfunction.....	16
3.3 Course of events in society	17
3.3.1 The disruption is discovered on a Friday	17
3.3.2 First weekday after the crash.....	18
3.3.3 Municipality resorts to Twitter	19
3.3.4 Problems across the country.....	21
3.3.5 Services return.....	21
3.4 The MSB's response to the incident.....	23
3.4.1 The MSB's formal points of reference.....	23
3.4.2 The MSB's activities	24
3.4.3 Contacts between Tieto and the MSB	26
3.5 Request for information in accordance with the Emergency Management and Heightened Alert Ordinance	27
3.5.1 Request to authorities in accordance with the Emergency Management and Heightened Alert Ordinance	27
3.5.2 Responses from governmental agencies with regional responsibilities	27
3.5.3 Responses from other governmental agencies indicated in the Emergency Management and Heightened Alert Ordinance	28
4. Analysis	31
4.1 New technology and business logic create new opportunities and social risks.....	31
4.2 National situation status reports in the event of major IT incidents.....	33
4.3 Comprehensive impact and handling assessment in the event of major IT incidents	35
4.4 Information coordination and communication.....	37
4.5 Emergency preparedness and contingency planning with a focus on information security.....	38
4.6 Risk analyses with a focus on information security.....	42
4.7 Learning from IT incidents	43
5. Final reflections and further work.....	45

5.1 Final reflections..... 45
5.2 Further work..... 46

**Appendix 1: Request in accordance with the Emergency
Management and Heightened Alert Ordinance (2006:942) 49**
Appendix 2: Privacy declaration 53

Summary

On Friday 25 November 2011, Tieto, an IT service company, suffered a technical error, which was to have a direct impact on about 50 of its customers both in the private and public sectors. The consequences varied considerably. Some customers got off lightly, with individual features knocked out for a few days. The worst affected basically lost use of their IT services for several weeks.

The increased concentration of IT operations and other IT related services, such as cloud computing, create new opportunities and also societal risks. This change in forms of delivery may be a way to both increase quality and reduce business costs. The incident shows that a disruption at a large IT operations supplier can affect an entire society and that the consequences can be considerable. Modern society continues to increase in sedentariness when IT systems become unavailable.

In order to prevent and manage major societal IT incidents, preventive information security must be strengthened further – at all levels of responsibility and across all sectors. This calls for greater collaboration between public and private actors. Special focus should be placed on risk analyses and contingency planning to support both procurement of IT services and to reduce the impact of IT incidents.

All societal actors must become better at using the power of procurement as a means of increasing their information security. For this to happen, however, a better understanding is required of how requirements are placed on security in agreements, as well as better access to advice and practical support. The overall procurement awarded by virtue of the Swedish Administrative Services Agency is an important tool for increasing information security in public administration.

In the event of IT incidents, warnings come at short-notice or not at all, the pace is rapid and the incident is usually geographically independent. The increased concentration of IT operations, and other IT related services, means that a large number of actors can be affected simultaneously by the same incident, and that societal impact can be severe. This places ever increasing demands on coordination and cooperation.

Cooperation and coordination of a major IT incident assume that there are relevant and current situation status reports at local, regional, sector and national levels. The disruption at Tieto shows that actors in the Swedish emergency management system need to enhance their capacities for situation status reports and overall impact and handling assessments. Stakeholders need to create processes for information gathering and information sharing. This should also include the ability to communicate information to citizens, which

requires information coordination. A system for mandatory IT incident reporting must also be developed.

1. Introduction

The disruption at IT operations supplier Tieto in November 2011 affected a large number of major societal actors in several sectors and resulted in several long-term disruptions. The impact of the disruption was nationwide, cross-sector and in several cases affected critical societal functions.¹ Therefore, the Swedish Civil Contingencies Agency (MSB) carried out a number of activities in accordance with the Agency's instructions. One of the **Agency's** main tasks is to create and maintain situation status reports, in addition to supporting and organising societal information security efforts, which also involves reporting to the Government on circumstances that may require action.

This report has been produced to describe the possible societal impact of a large-scale disruption in IT operations. The purpose is not to provide a detailed description of the Tieto disruption. Nor is the purpose to provide an exhaustive account of exactly which organisations were affected or to what degree those organisations were affected; doing so would be impossible, since no single actor has access to that information.

The focus has instead been on the impact for various societal functions and on the lessons that can be learned regarding emergency management – both from the perspective of individual organisations and from a societal perspective. This approach aims to strengthen society's ability to prevent and manage similar events. In other words, focus is **on society's** information management (information security) rather than on the technical conditions for such information management (IT security). It is thus a question of modern society's ability to withstand and recover from technical collapses such as the Tieto disruption, i.e. social resilience.

The proposals for continued work given in this report do not aim to treat technical development as such or to influence the direction of administrative development. However, the conclusions suggest that there are factors related to information security that may have a strong effect on the security and stability of e-administration.

Another issue that does not fall within the scope of this report is the socioeconomic cost of the disruption.

¹ For a discussion on critical societal functions, see *A functioning society in a changing world: The MSB's report on a unified national strategy for the protection of vital societal functions*. Publication number: MSB266 - December 2011, MSB. (<https://www.msb.se/RibData/Filer/pdf/26084.pdf>).

2. Background

2.1 Increased concentration of IT operations and IT related services

In recent years, accumulating IT operations in a central operational environment has become a common practice for both privately owned companies and the public sector in both Sweden and abroad. The environment is usually in the form of one or more data centres. For a number of years, many different types of equipment with various attributes and operating conditions have been replaced by virtualised server environments. In connection with these, data storage has also been centralized to storage networks. This change has resulted in cost advantages and streamlined administration.

Increased technical complexity, high establishment costs and rapid technological development have led to significant economies of scale for IT operations. As a result, additional cost advantages can be obtained by outsourcing all or some IT operations to one or more suppliers.

An increasing number of Swedish organisations are outsourcing their IT operations in this manner. This segment of the IT industry is dominated by large companies, one of which is Tieto.²

There is also the current development of IT related services, such as cloud services, where an organisation can choose to put a supplier in charge everything from storage of information to very advanced services. Like pure outsourcing of IT operations, the use of IT related services results in a concentration of information management.

This development is not unique to Sweden. It is an international trend that has been identified by the **Swedish National Audit Office's** American counterpart, the U.S. Government Accountability Office (GAO)³, amongst others. In other words, it is natural for the public sector to apply such solutions to utilise resources as efficiently as possible as well. This trend is also in line with the Swedish Government's general objective to be a world leader in terms of utilising the opportunities afforded by digitalisation.⁴ Through rational

² One way to determine who the major actors are is to examine the IT related framework agreements signed by the Swedish Legal, Financial and Administrative Services Agency. Hosting services are purchased as call off orders from Compose IT System (CITS) AB, Cypoint IT Services AB, EDB Business Partner Sverige AB, IBM Svenska Aktiebolag, IDENET AB, Office IT-Partner i Sverige AB, Obranch Stockholm AB, TeleComputing Sweden Aktiebolag, Tripnet Aktiebolag and Volvo Information Technology Aktiebolag. Overall operation is purchased as call off orders from CSC Sverige AB, EDB Business Partner Sverige, Fujitsu Sweden AB, Hewlett-Packard Sverige AB, IBM Svenska Aktiebolag, Logica Sverige AB, Obranch Stockholm AB, SYSteam Outsourcing Services AB, TeleComputing Sweden Aktiebolag and Tieto Sweden AB.

³ *Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of representative: INFORMATION SECURITY - Additional Guidance Needed to Address Cloud Computing Concerns.* Statement of Gregory C. Wilshusen, Director, Information Security Issues, Thursday, October 6, 2011 (www.gao.gov/new.items/d12130t.pdf).

⁴ *ITC for Everyone - A Digital Agenda for Sweden*, Swedish Ministry of Industry, Employment and Communications 2011, Journal number 2011/342/ITP, and the Government's budget proposal for 2012 (Bill 2011/12:01).

resource utilisation and different types of e-services, Sweden is to take the lead as regards improving efficiency in national and local administration.

In addition to the technical development, there have also been significant changes in societal structures. Private organisations are increasingly being commissioned by public buyers to perform operations that were previously carried out by public actors. This change of roles has affected public administration, both for individual organisations and at the national level.

In their role as customer, public actors regulate the distribution of security-related responsibility with suppliers through contracts. Therefore, public actors must be active parties to the contract and insist on including security aspects in their procurement processes, including everything from risk analyses to specific requirements. For critical societal functions, this is especially important since the requirements may include deliveries that affect civil protection and emergency preparedness.

2.2 Sweden's emergency management system

Sweden's emergency management is based on collaboration. All actors must be able to act together and collaborate with regard to decisions and initiatives in the event of an emergency. This applies to all regions and areas of business: the private sector, the Police, the fire and rescue services and decision-makers in municipalities, county administrative boards, governmental agencies and the Government. The emergency management system includes sector responsibility, geographic responsibility and operational responsibility divided into municipal (local) level, county administrative board and county council (regional) level, and governmental agency and government (national) level.⁵

An emergency is initially handled in its immediate vicinity, while regional and national resources stand by in case the events become too extensive to handle locally. This means that municipal operations form the basis for basically all emergency management. During an emergency, the county administrative board has overall geographic responsibility on regional level and provides support to the municipality in terms of collaboration between governmental agencies, municipalities and other actors. The county administrative board's support does not affect the responsibilities of other actors in managing the emergency.

Three important basic principles of the Swedish emergency management system are the principles of responsibility, equality and proximity.

The responsibility principle stipulates that the actor responsible for the operations during normal conditions is to retain that role during an emergency situation, also regarding initiating and pursuing collaboration.⁶

The equality principle stipulates that organisations are to retain their functions in the event of an emergency – to the extent possible. In addition, when

⁵ See for example: <https://www.msb.se/sv/Forebyggande/Krisberedskapssystemet/>

⁶ Bill 2007/08:92 Reinforced emergency preparedness – for safety's sake.

possible, activities are to be carried out at the same location as during normal conditions.

The proximity principle stipulates that an emergency is to be managed at the source by the parties who are most immediately responsible and affected. Regional and national initiatives are not to be launched until it is evident that local resources are insufficient.

3. Course of events and societal impact

3.1 General description

On Friday, 25 November, a hardware error occurs at IT operations provider Tieto. A central part of a large data storage system at a facility in Stockholm suffers an emergency shutdown. First, an important key component of the system is lost. At that moment, it would still be possible to fall back on a backup system that is on standby and ready to take over. However, after a short while the backup system malfunctions as well, thereby rendering data storage for the connected server systems non-functional.⁷

The exact details of what happened have not been made public by Tieto, but data storage for a large number of servers was suspended in a very short period of time. The disruption affects around 50 of Tieto's customers, including companies, governmental agencies and municipalities. Exactly which clients were affected by the disruption has still not been made public by Tieto. However, it is known that some of the affected parties include Apoteket AB, Apotekens Service AB, Bilprovningen (the Swedish motor vehicle inspection company), SBAB, the Swedish Research Council, Nacka Municipality, Sollentuna Municipality, and the City of Stockholm. For some organisations, IT support came to a near complete halt, while other organisations experienced disruptions of specific services. In addition, several service suppliers seem to have been connected to the storage system, including companies that deliver web-based tools for administration, travel management and similar services. There are reports from several municipalities across the country about malfunctioning administration of financial services and pension services following the disruption at Tieto.

It is difficult to provide an exact account of the direct impact of the breakdown, such as the number of IT services or servers that went down. However, it is possible to get a rough idea of the extent based on the outsourcing contracts between Tieto and some of the affected organisations. For example, one of the affected municipalities, Sollentuna, has transferred 14 employees and about 130 servers to Tieto. Nacka has transferred IT operations and 4 employees to Tieto. Bilprovningen has transferred IT operations and 15 employees to Tieto, and 10 persons from a large logistics company that was impacted have been transferred to Tieto. The disruption affected about 50 customers. The storage system crash resulted in the malfunction of a large number of servers, or virtual servers, in a short amount of time.

Moreover, the effects were not limited to the systems operated by Tieto. The company also sells automated operational monitoring of customer servers. As a result, several Tieto customers quickly noticed that they no longer had any

⁷ <http://www.tieto.se/press/driftsstorningar/fragor-och-svar>

control over the status of their own servers. This meant that they had to quickly move to manual monitoring, which resulted in a significant amount of extra work.

At least two municipalities in the Stockholm region, namely Haninge and Södertälje, were affected when operational monitoring crashed in conjunction with Tieto's storage system disruption. From previously having nearly instantaneous monitoring of their systems, these customers were forced to quickly arrange manual controls, which can only be made at sparse intervals. One municipality suffered extensive consequences as a result. During the time of the disruption, a number of functions connected to the **municipality's** central e-mail system crashed, and manual monitoring did not detect the malfunction in time. As a result, these functions were down for several days.

3.2 The technical malfunction

The technical malfunction at Tieto affected a central component of the data storage equipment, which means that basically all data storage for affected customers stopped functioning within a short amount of time. Besides the fact that the malfunction could be traced to a central part of the storage system, Tieto has not released any detailed information regarding the hardware error that caused the problem. The malfunction occurred on Friday, 25 November. The actual error took two days to correct, which means that the supplier's equipment was working again on Sunday, 27 November.

However, customer information, i.e. the data stored in the storage system, could not be restored simply by replacing a single component of the technical equipment because the hardware problem caused a chain reaction of incidents that resulted in a complex and time-consuming restoration process. Therefore, it took a considerably longer time for customers to restore saved data to the same state as before the disruption.

Data storage systems such as the one operated by Tieto constantly upload and download an enormous amount of data. The system consists of an entire network in the operations centre – a storage network – which is directly connected to the servers to retrieve and store data quickly and efficiently, without competing with other data traffic.

The storage network processes all data to and from databases, operations systems, web services, websites and other components of customer servers. After a short intermediate storage phase, data is placed on a large number of hard disks, tape memories and other storage devices in accordance with a complicated schedule.

A functioning storage network is integral for the functioning of servers and critical for all of the services handled by Tieto on behalf of its customers. When the storage network stops working, it only takes a few moments for the data in the storage space to become outdated, rendering the stored data corrupted. In order to restore all data and resume normal operations, access to backup copies is required.

3.3 Course of events in society

The following section is based on the information that the MSB has gathered on the shutdown at Tieto. The summary of the course of events is not intended to be exhaustive.

3.3.1 The disruption is discovered on a Friday

The disruption at Tieto occurred on a Friday afternoon and the supplier soon realises that something serious has happened. The internal emergency organisation at Tieto is activated and attempts to correct the malfunction. Since many of the customers mainly operate on weekdays, there is an opportunity for Tieto to limit the damage by correcting the immediate cause of the malfunction over the weekend, which the company succeeds in doing.

However, several customers have experienced major problems, as they operate around the clock. Over the weekend, the Tieto disruption had started to gain national media attention, mainly due to the fact that around 350 of Apoteket AB's pharmacies across the country suddenly lost contact with their IT systems and were unable to dispense prescribed medicines in accordance with normal routines.⁸

It is not yet known if the shutdown of the prescription management system caused any patient injuries, but many pharmacies found the incident to be of considerable inconvenience, especially hospital pharmacies and pharmacies in sparsely populated areas. Some pharmacies decided to administer their prescriptions manually, while others were able to install an older IT system rather quickly and were thus able to maintain their services.

A closely related organisation, Apotekens Service AB, is also affected by the Tieto disruption. The company's external website is down over the weekend as well as the entire following week. The website is an important source of information for the medical and health care sector in Sweden. It contains information about pharmaceuticals, contact information and information about disruptions. The company's other services, however, can be maintained since it had previously been decided that all critical services are to be handled in self-contained redundant environments.

The Government-owned mortgage lender SBAB is also affected by the disruption. In this case, the incident became critical as early as on Friday, as it happened to be on the 25th of the month, which is a common pay day. The banking and finance sectors traditionally consider this to be a sensitive time period, since disruptions can have a major impact. However, the company manages to limit the damage, and customer access to liquid assets is not significantly affected. On the other hand, the disruption has a large effect on SBAB's loan operations, which are not restored until the following Wednesday.

⁸ *Vissa av Apoteket AB:s apotek har för närvarande problem att lämna ut receptförskrivna läkemedel, (Some of Apoteket AB's pharmacies have problems dispensing prescription medicine), 27/11/2011,*

http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/vissa-av-apoteket-ab-s-apotek-har-foer-naervarande-problem-att-laemna-ut-receptfoerskrivna-laekemedel-709363

Another financial actor also experiences problems. For example, there are problems with the **company's** customer service, the production of credit cards is temporarily halted and payments to customer accounts cannot be monitored. In this case, the company is saved by backup copies and can relatively quickly resume normal operations.

A large logistics company is also among those affected. The company maintains large delivery contracts with the public sector, and the disruption prevents communication with customers via e-mail or via the internal and external websites, for example. The company quickly realises the potential risk of a prolonged disruption and promptly organises a crisis group. One circumstance that facilitates the process is that the company has previously experienced a major emergency situation and has therefore produced a contingency plan, which facilitates the work significantly.

Tieto does not acknowledge that it is experiencing operational problems caused by a hardware malfunction until Sunday afternoon, 27 November. Early Sunday evening the newspaper *Nacka Varmdö Posten* reports that Nacka municipality is experiencing problems with its website due to the **municipality's** IT supplier. The reports would prove to be merely a small indication of what would follow twelve hours later on Monday morning, when workers across the country arrive at work to find that the IT services that had functioned as late as Friday no longer work.

3.3.2 First weekday after the crash

Early Monday morning, 28 November, the mass media and the public have already started to understand the widespread impact of the disruption. The information from the supplier is, however, still very limited and the clearest indication of the disruption is the widespread effect.

As Monday drew closer, emergency management at the large logistics company escalated. By Monday morning, the situation at the organisation had become critical. Without IT support, the company cannot operate, and on Monday the company cannot even convey information to most of its employees. As an emergency solution, the company uses text messages to alert employees, which temporarily rectifies the situation. In addition, the company decides to prioritise customers in the public sector and to set aside other operations. This prioritisation is made in accordance with what the company's management considers to be critical societal functions. The management states that business needs have been set aside due to the gravity of the situation.

Bilprovningen (motor-vehicle inspection company) is at a standstill on Monday.^{9 10} Bilprovningen inspects around 5.5 million vehicles every year,

⁹ *Driftstörningar* hos Tieto kan skapa förseningar hos Bilprovningen, (*Disruptions at Tieto could cause delays at Bilprovningen*), 28/11/2011,

http://www.bilprovningen.se/extern/tpweb/about.nsf/va_LookupWeb/55A5618F0F97DA2EC125781500389CF9!OpenDocument&m=0

¹⁰ *Driftstörningar hos Tieto påverkar möjligheten att registreringsbesikta fordon*, (*Disruptions at Tieto affect the ability to inspect vehicles*), 28/11/2011,

http://www.bilprovningen.se/extern/tpweb/about.nsf/va_LookupWeb/55A5618F0F97DA2EC125781500389CF9!OpenDocument&m=0

which means that about 20,000 vehicles per day go through control stations across the country. All of a sudden, IT support is unavailable; only the telephones continue to work. Inspectors at 180 control stations across the country must quickly revert to manual registration of inspection results using pen and paper. This naturally slows down the inspection process and leads to extensive extra work and costs for post-registering the data.

Regular operations at the Swedish Research Council are halted completely when the governmental agency is affected by a near complete halt in IT support. The financial system stops working, the e-mail service is gone, and the agency's web services are unreachable. The application system, which is the case management system that handles research applications and reviews, is also unavailable. In order to communicate with the outside world at all, the Swedish Research Council has to create a temporary blog on the Internet.¹¹

3.3.3 Municipality resorts to Twitter

One of the municipalities in the area surrounding Stockholm, Nacka Municipality, experiences similar problems.¹² All municipal activities and operations are affected by the disruption at Tieto, from finance to education and municipal health and medical care. Furthermore, the website disappears as well and e-mail cannot be used to communicate within the municipality. All these services have been outsourced to the IT operations supplier. Communication with the public, the county administrative board and goods and services suppliers is gone. The municipality is forced to switch to social media such as Twitter and Facebook to somehow handle communication with citizens and partners.

Later during the day on Monday, the mass media begins to cover the incident more extensively, and social services in Nacka Municipality are forced to announce delays in financial support payments as a result of the disruption. The municipality is forced to temporarily switch over to manual payments.

During the day, the mass media also starts to speculate about the extent of the impact and who has been affected. The publication *Ny Teknik* publishes a long list of governmental agencies that are Tieto customers and which could thus be affected – a list that is also used by other media outlets.¹³ The information, however, is not particularly accurate. It was collected from a website that publishes information based on government invoicing and which is not limited to customers of IT operation services. For example, the Swedish Civil Contingencies Agency (MSB) is listed as a customer, as the Agency has purchased document templates for project management from the company.

Just north of Stockholm, in Sollentuna Municipality, the social services office has run into the same problems encountered in Nacka, and the municipality is

¹¹ <http://vetenskapsradet.wordpress.com/2011/12/05/vara-it-system-fungerar-igen-men-e-post-och-ansokningar-kan-vara-drabbade/>, posts on 28, 29 and 30 November, 1 and 5 December.

¹² *Störningar i Nacka kommuns IT-system, (Disruptions in Nacka's IT systems)*, 2011-12-12, <http://www.nacka.se/web/Nyheter/Sidor/Nackasefungerarigen.aspx>

¹³ *Stora mörkertalet när Tieto havererar, (Large number of unrecorded cases after Tieto crash)*, Ny Teknik 28/11/2011, http://www.nyteknik.se/nyheter/it_telekom/allmant/article3355166.ece

forced to pay financial support manually.¹⁴ It is later becomes clear that at least one additional municipality, Kalmar, has experienced the same problems and been forced to make manual financial support payments.¹⁵

In Sollentuna, operations are not halted completely, but a large number of government services are rendered unavailable. Among other things, municipal schools are experiencing major problems.¹⁶ The e-mail services no longer function and system login is impossible meaning current projects cannot be accessed. About 6,000 students and teachers are forced to use textbooks, pen and paper as substitutes. Sollentuna's public school system is extensive and has one of Sweden's largest secondary schools, for example.

Large parts of municipal administration in Sollentuna are affected when administrators suddenly are unable to work on their cases.¹⁷ Several systems depend on links to the file system, and consequently stop functioning. Along with the payment problems, the social services offices cannot access records, meaning that all applications for financial support have to be handled manually. Documents and data files in the administration system cannot be accessed, which creates delays in processing building permits, cases at the chief guardian's office, and cases relating to food, health and the environment.¹⁸ Minutes from the municipal council and the municipal executive board are delayed, parking permits for the disabled cannot be issued,¹⁹ monthly closing of the books is delayed and sport organisations cannot book facilities. In addition, the downtime means that all access to municipal facilities has to be administered manually.

Even the City of Stockholm is affected by the disruption at Tieto. The disruption primarily affects the city's website (www.stockholm.se) and its internal intranet. Although www.stockholm.se can be accessed, the website experiences disruptions. The intranet is at times down completely. However, the city's internal users are able to work as usual during the disruption, and the municipality does not consider the problems to be critical.

Stockholm's online service for school results, absence reporting and contact with legal guardians is shut down completely during the entirety of the disruption. It is not operational again until Thursday, 1 December. The recruitment tool "Jobb i stan" is also affected and is down until the evening of 30 November. During the downtime, application documents have to be submitted by other means.

14 *Problem med utbetalningar av ekonomiskt bistånd, (Problems with financial aid payments)*, 30/11/2011,

<http://www.sollentuna.se/Nyheter/Nyheter/Omsorg--socialt-stod/Asa-Hinndal-Anrin/>

15 *Dataproblem stoppar betalningar, (Data problems halt payments)*, Sveriges Radio, 29/11/2011,

<http://sverigesradio.se/sida/artikel.aspx?programid=86&artikel=4828825>

16 *IT-störningar påverkar skolan, (IT disruptions affect schools)*, 30/11/2011,

<http://www.sollentuna.se/Nyheter/Nyheter/NYHET---Barn--utbildning/IT-storningar-paverkar-skolan/>

17 *Stora IT-problem i Sollentuna kommun, (Serious IT problems for Sollentuna)*, 30/11/2011,

<http://www.sollentuna.se/Nyheter/Nyheter/NYHET---Om-kommunen/Stora-IT-problem-i-Sollentuna-kommun/>

18 *IT-störningar på miljö- och byggnadskontoret, (IT disruptions at municipal office)*, 30/11/2011,

<http://www.sollentuna.se/Nyheter/Nyheter/NYHET---Bostad--miljo/IT-driftstorningar-pa-miljo--och-byggnadskontoret/>

19 *Problem med tillverkning av P-tillstånd, (Problems producing parking permits)*, 30/11/2011,

<http://www.sollentuna.se/Nyheter/Nyheter/Trafik--teknik/Problem-med-tillverkning-av-P-tillstand/>

3.3.4 Problems across the country

The disruptions are, however, not limited to Stockholm and the municipalities in the surrounding area. There are reports of problems caused by the disruption from around the country. In Flen, the **municipality's** self-service system which handles employee time sheets goes down. This leads to an increased workload for the personnel department due to manual reporting and some instances of information being reported twice. In addition, it later becomes clear that certain data have been lost completely. In Vingåker, the payroll department is showered in phone calls after the payroll system shuts down, which also means that an associated self-service function is rendered unavailable.

In Skinnskatteberg in Bergslagen, bank giro service files can no longer be sent. Further south in the country, Kalmar Municipality experiences problems with financial systems as well as indirect problems with payroll systems and social services systems. Payment of salaries and financial support is delayed, suppliers are not paid on time and incorrect payment reminders are sent.

In Nyköping Municipality, processing of service pensions stops completely for four or five days as a result of the disruption. However, the disruption only affects service pension processing, and the impact is thus regarded as minimal. However, pension problems are not limited to Nyköping. Further south in Sweden, a county council reports similar problems with the same service.

The disruption also affects the Nationell Patientöversikt (NPÖ) service at the Swedish health care sector's common IT infrastructure company Inera AB. NPÖ is a comprehensive health care information system that includes medical record functionality. **The system is gradually being introduced in Sweden's** medical care system. After the disruption, the testing environment and demonstration system used for NPÖ suddenly become unavailable. According to Inera AB, the disruption primarily affects health care providers that are about to introduce the system and that are training their staff to use it. Inera AB states that the production environment for NPÖ does not seem to have been affected by the disruption.

It appears that most of the affected customers continue to experience problems during the entire weekend of 26-27 November and the following Monday, 28 November, even though the immediate cause of the problem has been corrected by Sunday. The restoration of customer data is apparently time-consuming, and judging from the growing number of reports published by the mass media on Tuesday, it is taking time for the IT operations supplier to restore normal operations for customers.

3.3.5 Services return

One of the first major customers to regain IT support in parts of its operations is Apoteket AB. However, around half of the affected pharmacies are not back in operation until Monday evening.^{20 21} At this point, Tieto has allocated

²⁰ *IT-problem kvarstår i hälften av Apoteket AB:s butiker, (IT problems remain at half of Apoteket AB's pharmacies).*

28/11/2011, http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/it-problem-kvarstaar-i-haelften-av-apoteket-ab-s-butiker-709582

additional resources to restore operations at Apoteket AB, since they are considered to be critical societal functions. It is worth noting that this was not a decision made by an underlying societal actor, but a decision by the IT operations supplier to prioritise the pharmacies. On Tuesday, Tieto has managed to restore operations, and around midday on Wednesday, Apoteket AB announces that all pharmacies are up and running again.²²

Bilprovningen's operations are not restored until later that week. The first thing to be restored is the company's e-mail, which is back online on Tuesday – after about 4 days of downtime. Other functions stay down longer. Overall, the disruption affects **Bilprovningen's** activities around the country for the entirety of the following week.

One notable consequence of the shutdown at Bilprovningen is that the automatic reporting of all approved inspections normally made to the Swedish Transport Agency was halted. This may seem trivial, but it triggered a driving ban for many vehicles since Bilprovningen could not report approved inspection results.²³ Only after ten days have passed, on the morning of 5 December, Bilprovningen announces that the company's control stations once again have IT support, and that inspections and bookings will resume normal operations.

It takes almost a week to restore normal operations for the City of Stockholm. Tieto contacts the City of Stockholm early on Saturday, 26 November, and the parties continue to maintain a close dialog. At the request of the city, Tieto stays in direct contact with affected system owners. During the first half of the following week, system environments are restored and the City of Stockholm concludes that there are no lingering effects of the disruption after Thursday, 1 December.

IT operations are down for eleven days at the large logistics company, and even 2 months after the initial incident, the company claims not to be back to normal conditions.

The situation is complicated in Nacka Municipality as well, and the website is not operational again until Wednesday, 30 November. Meanwhile, the municipality communicates with the outside world in other ways. One week after the disruption, several central IT systems in Nacka are still out of service. Documents and protocols are unavailable, functions for municipal error handling fail to work and the e-authentication login service is down.

²¹ *Fortsatta IT-problem i Apoteket AB, (Continued IT problems for Apoteket AB)*, 28/11/2011,

http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/fortsatta-it-problem-i-apoteket-ab-709698

²² *Nu kan Apotekets kunder återigen hämta ut receptläkemedel på samtliga apotek, (Apoteket's customers can finally pick up prescriptions from all pharmacies)*, 30/11/2011,

http://www.mynewsdesk.com/se/pressroom/apoteket_ab/pressrelease/view/nu-kan-apotekets-kunder-aterigen-haemta-ut-receptlaekemedel-paa-samtliga-apotek-710514

²³ *Har du fått körförbud på ett fordon med godkänd besiktning?, (Has your car failed inspection after being approved?)*,

29/11/2011, <http://www.transportstyrelsen.se/sv/Nyhetsarkiv/Har-du-fatt-korforbud-pa-ett-fordon-med-godkand-besiktning/>

Nacka is not able to announce 95% recovery of operations until the middle of December. All computer systems are not up and running again until 4 January. However, there is still a lot of catching up to do and the municipality has identified lost data. The cost caused by the shutdown is estimated to be at least SEK 7.5 million.²⁴

In mid-December, Sollentuna Municipality points out several lingering consequences of the disruption. The delay in administration will, for example, be difficult to compensate. Manual records must be entered electronically, which impacts daily work where other tasks risk not being completed. In addition, projects have been delayed in a manner that will be difficult to offset. Furthermore, the file area is difficult to restore to its previous state, which causes different file versions to be created. Links between files are broken and there have been time-consuming investigations since the shutdown to ascertain which links are broken.

3.4 The MSB's response to the incident

3.4.1 The MSB's formal points of reference

The MSB is responsible for matters relating to emergency preparedness and emergency management in the event no other governmental agency has already assumed responsibility. This is established by the Ordinance with instructions for the Swedish Civil Contingencies Agency (2008:1002):

Section 1 The Swedish Civil Contingencies Agency is responsible for matters relating to protection against accidents, emergency preparedness and civil defence, in the event that no other agency has already assumed responsibility. The Agency's responsibilities regard actions before, during and after an accident or emergency.

/.../

Section 7 The Agency must be able to contribute with support during serious accidents and emergencies, and support the coordination of affected governmental agencies' actions during an emergency. During an emergency, the Agency is to make sure that affected actors are able to

- 1. coordinate emergency management measures,*
- 2. coordinate information to the general public and the media,*
- 3. make efficient use of society's common resources as well as international resources, and*
- 4. coordinate support to central, regional and local bodies regarding information and situation status reports.*

The Agency must be able to provide the Government Offices with data and information during serious accidents and emergencies.

/.../

In addition, the instructions state that:

Section 11a The Agency is to support and coordinate the work on societal information security, and analyse and assess the global development in the

²⁴ *IT-haveriets kostnad hittills: 7,5 miljoner, (The cost of the IT crash to date :SEK 7.5 million),* Nacka Varmdö Posten, 24/01/2012, <http://www.nvp.se/Nacka/Nacka/IT-haveriets-kostnad-hittills-75-miljoner/>

field.

/.../

In addition, the Agency is to make sure that Sweden has a national function that supports society's work on preventing and managing IT incidents. As part of this work, the Agency is to

1. act promptly during IT incidents by spreading information and, when needed, coordinating and assisting the work to avert and minimise the incident's effects,

/.../

3.4.2 The MSB's activities

Sunday, 27 November

The MSB noted the disruption at Tieto at around 16.00 on Sunday, 27 November, when **the Agency's** Officer on Duty received a report on IT disruptions at Apoteket AB. Affected managers and emergency preparedness functions at the Agency were informed of the situation within 15-20 minutes.

Monday, 28 November

At 08.30 on 28 November, Nacka Municipality called and asked to publish information on www.krisinformation.se, as **the municipality's** website was not available. Krisinformation.se published the news at 09.00 and referred to Nacka's Facebook page. Meanwhile, the IT disruption was brought up during the MSB's daily staff briefing at 09.00, at the Agency's situation centre. Shortly thereafter, Nacka Municipality managed to launch a simple backup page with important information and phone numbers. After the staff briefing, the MSB's experts on information security began to search more actively for information on the issue. Among other things, the MSB contacted Tieto and some of the organisations affected by the disruption.

Apoteket also asked to publish information on Krisinformation.se. The editorial office put up a special page about the disruptions, with references to external sources (including Krisinformation.se's Facebook and Twitter channels) that the general public could turn to for information. This resulted in many visits to the website and questions from the public. Krisinformation.se reported to the Officer on Duty regarding contacts and questions from various actors and the public. **The MSB's** Officer on Duty reported on the event in the **Officer's** daily contact with the Swedish Ministry of **Defence's** Officer on Duty.

It became quickly apparent that Bilprovningen had been affected as well, that a large number of Tieto customers were governmental agencies, and that the event could potentially have more widespread consequences. It was also clear that no other public actor at the national level had any intention of taking direct action. Consequently, it was decided shortly after 10.00 to mobilise the National Cybersecurity Coordination Function (NOS)²⁵. The first meeting was

²⁵ The National Cybersecurity Coordination Function (NOS) was established by the MSB to address serious IT incidents systematically. The function is still being developed, and is gradually being built up within the MSB in collaboration with other societal actors.

held at 10.45, where a decision was made to produce an initial situation status report on information security by 12.50, as well as to contact affected parties within the **MSB's** established networks in the area of information security. At a meeting at 12.50, the situation status report was presented along with a report on contacts.

During the afternoon, analytical work continued and was compiled into a situation status report on information security at 16.30, and then presented to those affected. At all of these meetings, **it was discussed whether the MSB's** National Management Plan for Major IT Incidents should be activated, but it was ultimately deemed unnecessary. See more in section 4.3.

Tuesday, 29 November

On Tuesday, 29 November, a staff briefing on the situation was first held, followed by formal meetings in NOS at 11.50 and 15.00. On Tuesday, the MSB was also contacted by the mass media regarding the events **and the MSB's role**. Information on the events was published on the MSB's external website at lunchtime on Tuesday, and the manager in charge participated in several interviews throughout the rest of the week.

The MSB carried out an impact analysis and concluded that no critical societal functions were affected in such a way that would seriously threaten the functioning of society. The critical societal functions that were deemed to be affected included the supply of medicines, caused by Apoteket AB's disruptions, as well as payment of financial support, caused by disruptions in certain municipalities. Information from involved actors indicated that operations, despite disruptions, were functioning at a satisfactory level due to alternative routines. Other known consequences were deemed as not seriously damaging the functioning of society or the lives and health of the general public. Since it was difficult to obtain information regarding which Tieto customers were affected, it was deemed possible that reports of additional critical societal functions that were affected could be received in the coming days.

Wednesday, 30 November through Friday, 9 December

During Wednesday, 30 November, a preliminary situation status report was completed for the Swedish Ministry of Defence.

On Wednesday, the MSB's Officer on Duty was in contact with the County Administrative Board of Stockholm, the Swedish Post and Telecom Authority and the Swedish Financial Supervisory Authority to assess the situation within their respective areas of responsibility.

Formal meetings within the framework of NOS were held on Friday 2 November, Monday 5 December, Tuesday 6 December and Friday 9 December at which on-going contacts were reported and the situation status report could be supplemented. At the meeting on Friday, 9 December, a decision was made to deactivate the National Cybersecurity Coordination Function (NOS) and to continue the investigation under normal working conditions.

However, the Agency lacked an overall understanding of the societal impact, and on Monday, 5 December, the MSB decided to ask governmental agencies with particular responsibility in accordance with Section 15 of the Emergency Management and Heightened Alert Ordinance (2006:942) to account for the impact of the disruption within their respective areas of responsibility. The request was prepared on Monday and finished and dispatched on Tuesday, 6 December; see Appendix 1 and section 3.5.

3.4.3 Contacts between Tieto and the MSB

As mentioned above, the MSB contacted Tieto directly at a very early stage in order to gain a better understanding of the situation. The company was willing to meet with the MSB, but informed the Agency that the exact technical problems that caused the disruption or which customers were affected could not be revealed due to commercial confidentiality reasons. A requirement for providing the MSB with any new information was that the Agency, as well as the officers receiving the information, would sign a non-disclosure agreement. The agreement would prevent the information from being spread outside of Tieto's control. This practice is established and logical between private parties, but for a Swedish governmental agency, such an agreement contradicts the principle of public disclosure that requires the release of general information to be tried on a case by case basis when access is requested. The agreements, especially with the officials involved, could potentially contradict the constitutional freedom of information. The MSB does not have a supervisory board mandate or the equivalent to request information from private actors in these situations, and is thus completely at the mercy of each private **actor's** willingness to provide information.

The problem was temporarily resolved with a privacy declaration drafted by lawyers at the MSB. This declaration described the legal requirements of an Agency, as well as the sections of laws that may be used to protect sensitive information received and that could potentially result in financial loss or other damage if shared. For more information, see Appendix 2. The company asserted that it under these circumstances could not disclose written information, but could share information in special reading rooms on its own premises.

Tieto offered to include the MSB as an external party **on its** "commission of inquiry", which was started around the turn of the year. Initially, the MSB participated along with the Swedish Medical Products Agency, the Swedish Financial Supervisory Authority, and the Legal, Financial and Administrative Services Agency as well as a number of customer representatives, as part of a reference group created by Tieto for the two consulting firms responsible for investigating the shutdown.

The MSB has assessed that it has gained very little new information that was not already generally available through its participation with Tieto; a view shared by the Legal, Financial and Administrative Services Agency.

At the meeting that took place with the reference group for Tieto's commission of inquiry on 16 January, nothing new was revealed. Tieto's representatives

stated that they did not want to disclose any information until the commission of inquiry's work was complete. Following this meeting, the Legal, Financial and Administrative Services Agency announced that it had no intentions of continuing its participation in the reference group.

The MSB, however, deemed that there was reason to continue monitoring Tieto's **commission of inquiry's** work as a means of potentially gaining additional information. Therefore, the MSB participated in additional meetings. During these meetings, information on the course of events and impact that had previously been unknown were revealed.

3.5 Request for information in accordance with the Emergency Management and Heightened Alert Ordinance

3.5.1 Request to authorities in accordance with the Emergency Management and Heightened Alert Ordinance

During the week following the disruption, the MSB followed the progression of events through open sources, its own contact networks and contacts with affected parties. The MSB quickly contacted Tieto, as well as many of affected organisations previously mentioned. However, it was difficult to gain complete understanding of the situation from the perspective of societal considerations through these channels as regards the widespread effects of the disruption.

Therefore, a request was drawn up on 6 December²⁶ for the majority of agencies specifically indicated in the Emergency Management and Heightened Alert Ordinance (2006:942) to submit a situation report to the MSB regarding the disruption at Tieto. The 36 agencies to which the request was submitted included: the Swedish Data Inspection Board, the Swedish Energy Agency, the Swedish Financial Supervisory Authority, the Swedish Coast Guard, the Swedish National Food Agency, the Swedish Medical Products Agency, the Swedish Post and Telecom Authority, the National Police Board, the Swedish Meteorological and Hydrological Institute, the National Board of Health and Welfare, the Swedish Radiation Safety Authority, Svenska Kraftnät (the Swedish National Grid), the Swedish Transport Administration, the Swedish Transport Agency and Swedish Customs, as well as all 21 county administrative boards.

In addition to the agencies included in Section 15 of the Emergency Management and Heightened Alert Ordinance, a request was sent to the Swedish Armed Forces.

3.5.2 Responses from governmental agencies with regional responsibilities

The County Administrative Board of Gävleborg stated that one municipality has informed the Board of problems at an institutional kitchen as a result of the

²⁶ Request regarding information about disruptions caused by the hardware malfunction at Tieto, MSB, journal number 2011-6477

disruption. The institutional kitchen could not receive orders for special diets. Another municipality reported communication problems between driving schools and the Swedish Transport Administration as well as the Swedish Transport Agency.

The County Administrative Board of Kalmar noted that Kalmar Municipality has experienced problems with its financial system, as well as with Apoteket AB's prescription service.

The County Administrative Board of Norrbotten stated that Swedavia AB has experienced problems with its telecommunication and transaction systems following the disruption at Tieto.

The County Administrative Board of Södermanland reported that three municipalities have experienced disruptions in their payroll management systems, but that those disruptions did not lead to any consequences for the general public.

The County Administrative Board of Västmanland stated that the Swedish Prison and Probation Service and Skinnskatteberg Municipality were affected by the disruption. The Swedish Prison and Probation Service experienced problems with supplying prescription medicines to its medical care units, which were connected to the disruptions at Apoteket AB. Skinnskatteberg Municipality also experienced problems with the financial office.

In regards to other county administrative boards, one board stated that "no actors known by the Board have been affected by any major consequences...", but it does not state where the non-major consequences were detected. Six boards pointed to indirect effects within their geographical area. One of them indicated Apoteket AB's and Bilprovningen's problems. One county administrative board said that Apoteket and some municipalities have been affected, but does not name the municipalities. Four boards only mentioned the problems experienced by Apoteket. Finally, one county administrative board stated that it was not affected, but emphasised that it did not assess the regional situation, but only its own operation

Two administrative boards did not provide the MSB with a response to the request.

3.5.3 Responses from other governmental agencies indicated in the Emergency Management and Heightened Alert Ordinance

The Swedish Medical Products Agency reported that a large pharmacy chain (Apoteket AB) that covers about one third of the country's pharmacies was affected. Prescription processing was shut down. The relevant individuals at the Swedish Medical Products Agency were informed of the disruption on the day that it occurred, and have since been informed that the stoppage has been taken care of. Lingering effects cannot be assessed at this time.

The Swedish Post and Telecom Authority did not note any disruptions in publicly available electronic communication networks or services in Sweden. However, the Swedish Post and Telecom Authority was to a lesser extent

affected by the disruption as a public service called "Test your computer" **went** down for a shorter period of time. The operation of this service is currently handled by Tieto.

The National Board of Health and Welfare stated that Apoteket AB was affected by the disruption.

The Swedish Radiation Safety Authority submitted a thorough report that reported no effects to self-contained, critical systems. The critical systems at nuclear facilities were not affected either. However, a system for handling supplier invoices at a nuclear facility's holding company was affected.

The Swedish Coast Guard, the National Police Board, the Swedish Data Inspection Board, Svenska Kraftnät, the Swedish Armed Forces, the Swedish National Food Administration and the Swedish Energy Agency reported no known impact from the incident within their respective areas of responsibility.

Five of the specifically requested authorities did not provide a formal response to the MSB's request.

4. Analysis

4.1 New technology and business logic create new opportunities and social risks

The disruption at Tieto emphasises an already known circumstance, namely that new technology has created new opportunities as well as new risks in our society. New technology and new business solutions have allowed a concentration of information, services, communication and IT operations in society. In the public sector, the trend towards concentration has been strengthened through a number of initiatives such as the eGovernment Delegation,²⁷ National eHealth,²⁸ the proposal for a common service authority,²⁹ as well as the framework agreements that the Legal, Financial and Administrative Services Agency has signed with major partners.³⁰

The increased concentration, along with new forms of operations and increased integration create a new category of vulnerability where technical errors can shut down a number of societal functions in a short period of time. Moreover, this makes it difficult for individual organisations to monitor the IT resources they depend on for their operations, something that is especially serious for critical societal functions.

The discussion surrounding information security has recently been focused on antagonistic threats, such as hacking attempts, cyber-crime or IT attacks with political motives. These phenomena represent an important dimension of information security, but are also just one part of the overall security problem. Disruptions caused by technical problems, natural events or human error are not as spectacular as intentional attacks, but can have a major impact on society. The disruption at Tieto confirms this fact. It should also be noted that the effects related to emergency management in society would to a large extent be the same if the incident had been an intentional attack, i.e. caused by criminal activity.

The disruption at Tieto was caused by a technical problem not described in detail in this report. In this context, however, the technical details are of minor interest. It is enough simply to conclude that different types of technical problems could lead to future IT incidents where important aspects of society are seriously affected.

²⁷ See, for example, SOU 2009:86 *Strategi för myndigheternas arbete med e-förvaltning*, SOU 2010:20 *Så enkelt som möjligt för så många* som möjligt, as well as SOU 2011: 67 *Så enkelt som möjligt för så många som möjligt – vägen till effektivare e-förvaltning*.

²⁸ *Nationell eHälsa – strategin för tillgänglig och säker information inom vård och omsorg*, S2010.020, Ministry of Health and Social Affairs.

²⁹ SOU 2011:38 *Ett myndighetsgemensamt servicecenter*, and Dir. 2011:99 *Tilläggsdirektiv till Utredningen Ett myndighetsgemensamt servicecenter för en effektivare statlig administration* (Fi 2010:08)

³⁰ See, for example, the Legal, Financial and Administrative Services Agency's procurement documents *E-förvaltningsstödande tjänster 2010* and *IT-driftstjänster 2010*.

The Government has pointed out how important it is that "the public sector knows how to procure solutions for secure information management and consequently how standards for information security are set".³¹ Security has been identified as a prerequisite for fulfilling the requirements set by citizens and the Government alike for developing e-administration, as well as for attaining advantages that e-services can provide for individual governmental agencies. Functioning security is a prerequisite for improved service and more efficient management with the possibility of economic rationalisation. Secure e-administration can entail advantages for the business world by facilitating e-commerce. Security for IT operations is also a current prerequisite for functioning communication with the public, during normal conditions as well as during an emergency.

If the public sector is to be able to reap the benefits that the market has to offer, it must be able to set requirements and exercise procurement adequately. Information security aspects must have a central role in setting requirements for coordinated framework procurement and single party procurement. This implicitly means that procurements must be preceded by different forms of activity analyses.

In this area, there are still shortcomings, a fact that the Swedish National Audit Office recently observed.³² In an audit of 95 governmental agencies, the National Audit Office concluded that the vast majority of them did not adequately assess whether self-contained or outsourced IT was most appropriate in terms of satisfying their needs. Shortcomings in the internal control of IT operations, inability to report IT costs, unclear information classification, intricate regulations surrounding public procurement and the lack of buyer competency are a few of the problematic areas pointed out.

The Legal, Financial and Administrative Services Agency's procurements are a central component in terms of combining the major functional and financial advantages found in technical development with a high level of information security in the long-term. Since the Swedish public sector has the option of basically carrying out all procurement of IT operations and supporting e-administration services via the Swedish Legal, Financial and Administrative Services Agency's framework agreement, there are good opportunities for including common security requirements.³³ Correctly designed, the security requirements in framework agreements can help organisations with limited competency in security issues choose the right level of security for the services being procured.

In conclusion, additional efforts are required for the public sector to take full advantage of the opportunities afforded by digitalisation. When outsourcing services, the preventive measures must be included in the procurement phase

31 *IT i människans tjänst – en digital agenda för Sverige*, journal number 2011/342/ITP, Ministry of Enterprise, Energy and Communications

32 *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?*, RIR 2011:4, the Swedish National Audit Office

33 Compare with the discussion about common requirements and developed procurement in the report titled *Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor, Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap (Fö2010/701/SSK, Government decision 12, 14/11/2010)*, journal number. 2010-6304, MSB

since it is normally both complicated and more expensive to add such measures at a later stage. This, however, requires awareness of the risks found in the relevant operations and a willingness to deal with such risks. Once this understanding is in place, a balanced decision can be made in regards to which risks can be accepted and which risks must be avoided.

4.2 National situation status reports in the event of major IT incidents

An emergency situation is characterised by a large number of information sources, as well as information recipients. Situational information is a prerequisite for all involved actors to understand and handle the situation. If the actors are to be able to plan measures together and allocate resources, situational information must be shared between the actors in order to gain a common understanding of the situation. Coordinated actions, in other words, require a common understanding of the current situation so that the actors can proceed in a coordinated manner when making decisions. This could, for example, be in a form of providing aggregate information to the public or jointly establishing a course of action.

It is of great importance to be able to quickly detect and present the progression of events in the case of major IT incidents. If the situation status report related to information security shows that many actors in society are affected at once, other action is required than if only certain individual actors are affected. Today, basically all emergencies have an IT dimension, which is why the MSB is joining the situation status report related to information security with the general national situation status report that the Agency is to produce and report to the Government.³⁴

The incident at Tieto showed that the necessary information collection needed for a situation status report on information security, and subsequently, a national situation status report, was difficult to carry out. In order for the MSB to disseminate information regarding IT incidents, as well as to coordinate and contribute to efforts to remedy or alleviate the effects of IT incidents, the MSB must have access to current and relevant information from different actors. High-quality information is also necessary in order to evaluate and draw strategic conclusions regarding the incident.

Tieto has confidentiality agreements with its customers and could not, due to such agreements, disclose information regarding which customers were affected by the IT incident. The MSB has no mandate to demand this type of information from private actors, and instead had to seek information through other sources. Even for sector authorities, the required instruments for quickly forming an understanding of what has occurred in the case of emergencies are not in place. In order to learn which actors were affected by the incident, the MSB collected and processed information from open sources, other governmental agencies and internal networks. Since this was not considered sufficient, a request was submitted in accordance with Section 15 of the

³⁴ For more information, see Section 7 of the Ordinance with instructions for the Swedish Civil Contingencies Agency (2008:1002).

Emergency Preparedness Ordinance to county administrative boards and other relevant governmental agencies. According to the request, governmental agencies were to submit information on possible effects of the incident.

The MSB can conclude that the fact that Tieto's information was very scanty regarding which actors were affected caused a long delay and a high level of uncertainty regarding which actors were affected and in what manner. It is noteworthy, however, that the MSB and the IT operations supplier in question initiated a dialog at an early stage. Tieto asserted, as previously pointed out, business confidentiality. In order to produce a situation status report that comprehensively described the societal impact of the incident, however, access to company information would not have sufficed. To create such a picture, information from a wide range of actors, including those that were affected and those that were not, as well as those indirectly affected would have been required.

The IT incident at Tieto had nationwide impact across several sectors, which required the MSB to contact a large number of governmental agencies quickly in order to gain a sufficient overview of the events. This can be compared with emergencies and incidents with geographically limited effects, such as floods and storms.

An important conclusion to note from the answers received by the MSB in response to its request for information is that many county administrative boards and governmental agencies lack routines for gathering this type of information for their respective regions or sectors. There were several cases where the reported information was the same as that reported by the mass media; in other words, the entity that was to report did not obtain any information on its own. Some actors misinterpreted the request and only provided information regarding their organisation as opposed to their sector or region.

During the disruption, informal contacts (networks) proved very useful. However, it is important to continue working with the established networks for information sharing when it comes to information security. The information networks rely heavily on trust between key people. Sick leave or other absence could, therefore, seriously reduce the prerequisites for sharing information at critical stages. The MSB has concluded that the formal process for gathering information, for example upon request in accordance with the Emergency Preparedness Ordinance, needs to be developed as regards IT incidents.

In the event of an IT incident, consequences can affect the areas covered by different governmental agencies, within which the rules for confidentiality may differ. Therefore, it is difficult immediately to see what type of information can be shared between different governmental agencies. The information that a governmental agency with supervisory responsibility gathers may, for example, be difficult to share for other purposes. Some governmental agencies have also pointed out that such sharing of information might damage the trust relationship with the organisations for which supervision is conducted. The Legal, Financial and Administrative Services Agency was not prepared for questions regarding which public organisations utilise framework services of a

certain supplier. Some information is, however, already available from the Legal, Financial and Administrative Services Agency. In addition, by requiring more statistics from suppliers, the authority could create updated lists of customer contracts.

The mass media and the Internet, certain discussion forums in particular, are fast news sources. However, there was some speculation and a great deal of discrepancies with regard to the disruption at Tieto. This is critical in itself since many organisations rely solely on these sources for information. One possibility is to increase the use of Krisinformation.se for spreading confirmed and coordinated information. Many governmental agencies, municipalities and other actors obtain information from the website, including the social media sources that Krisinformation.se offers and which function as fast disseminators of information. Central actors should increasingly have access to their own information. In cases where the situation status reports produced by various actors are based exclusively on mass media reports, source criticism is of crucial importance.

In summary, it can be concluded that the MSB had difficulty quickly creating a comprehensive picture of how the IT incident affected the Swedish society. There is currently no actor with a complete picture of the societal impact. The ability to assess situations is mainly applicable to consequences of significant importance to the function of society. However, some of this information is also difficult to gather. The conclusion is that there are formal limitations imposed on the MSB and other governmental agencies in terms of accessing relevant information.

4.3 Comprehensive impact and handling assessment in the event of major IT incidents

The disruption led to widespread damage at a large number of organisations, mainly concerning the availability of IT based services. The mass media has primarily highlighted the effect of the disruption on the availability of services provided by Tieto's customers, but it should be emphasised that other, not fully clarified consequences related to data loss occurred as well. Some actors have already reported data losses since they were forced to reset their systems to earlier versions. Others suspect data loss, but have no way of verifying it. The MSB's assessment is that the disruption could have caused even more serious societal impact had it occurred under different circumstances, such as earlier in the month or if it had affected payment of salaries and other transfers to a greater extent. The disruption could also have affected additional operations, leading to more serious impact, if for example, Apotekens Service AB's distribution system had been affected.

The disruption did not cause the MSB to activate its National Management Plan for Major IT Incidents.³⁵ This plan includes criteria for what is considered a major IT incident. Among other things, one requirement states that the event

³⁵ *Managing Serious IT Incidents: National Management Plan. Interim version, March 2011. Publication number: MSB328 - November 2011, MSB.*

must require quick and coordinated measures at the national level. The MSB did not find this to be the case during the disruption at Tieto. The simple fact that the MSB did not activate the management plan, however, does not mean that the situation was not considered to be "major", nor does it mean that critical societal functions were not affected, as has been discussed above. In terms of determining whether the incident was major or, perhaps, could be considered an emergency, it is important to distinguish between society's perspective and the perspective of individuals and organisations. In this respect, the disruption clearly had serious negative consequences for individuals and organisations, meaning the disruption was very serious. Government bills and official communication that have treated **society's** emergency preparedness the past few years have a definition for the term "emergency", as well as the term "exceptional event" for municipalities and county councils.³⁶ From this perspective, the consequences of the disruption at Tieto cannot be considered a social emergency, but possibly an exceptional event for a number of the affected municipalities. For comparison, please see the MSB's assessment of how **Sweden's emergency** preparedness functioned in periods of excessive snow in 2010.³⁷

An important process in the management of a major IT incident is the in-depth analysis of the impact and an assessment of how they are handled, including an assessment to determine whether there is a need for specific resources. The process of producing a comprehensive impact and handling assessment can be seen as part of an in-depth understanding of the situation and thus complements the situation status report as described above. In other words, it is the next step in creating a coordinated response to the event, and aims to create good opportunities for affected actors to coordinate measures and actions. A natural part of the impact and handling assessment is to provide recommendations and warnings to representatives of critical societal functions, as well as to the general public.

Currently, many critical societal functions use centralised IT services, either through commercial cloud services or national partner clouds. A more extensive disruption could, according to the MSB's assessment, have had a major impact on transport and health care, for example. It is, however, difficult to assess the impact of major IT incidents at the societal level, partly due to the complex dependencies being created by new technology, and partly since it is not entirely clear what is to be considered a critical societal function.

³⁶ **Emergency** has the following definition in official communication 2009/10:124 Samhällets krisberedskap – stärkt samverkan för ökad säkerhet: "An emergency is an incident that affects numerous people and large portions of society, and threatens basic values and functions. An emergency is a condition that cannot be managed with normal resources and organisations. An emergency is unexpected, and resolving it requires coordinated measures from several actors." This definition is also provided in Government Bill 2007:08:92 Stärkt krisberedskap för säkerhets skull.

Exceptional event is defined in the Act on municipal and county council measures before and during extraordinary events in peacetime and periods of heightened alert (2006:544): "an incident that deviates from the normal, which entails a serious disruption or imminent risk of a serious disruption in critical societal functions and which requires prompt action by a municipality or county council."

³⁷ *Perioder med stora snömängder vintern 2009/2010. Account of government assignment to analyse and assess how emergency preparedness has functioned during periods with excessive snow in the winter of 2010.* Publication number: MSB 0199-10, MSB

Centralised IT services also make it difficult for individual actors to gain an overview of these dependencies in their operations.

The disruption at Tieto clearly shows that information about certain actors being affected by the disruption does not automatically provide an insight into societal dependencies or an understanding of possible impact. In order to make a comprehensive impact and handling assessment of an on-going IT incident, cooperation between all affected actors is required. Today, coordination between private and public sectors is a prerequisite for managing all types of emergencies in society. In the event of more extensive IT incidents, the need for cooperation between the private and public sector is particularly prominent due to public actors' reliance on private service suppliers. Private actors need to participate in existing processes for cooperation and collaboration within the public sphere. In the assessment made after the national emergency test SAMÖ-KKÖ 2011, it is evident that there is reason to monitor the forms for who participates and how coordination of meetings should be structured in the initial phase of an emergency.³⁸

The MSB can establish that there were shortcomings among affected actors in terms of analysing impact and dependencies in connection with the disruption. Several of the affected actors do not have enough knowledge of their own dependencies, nor about their need for cooperation. Had the IT incident led to more extensive social problems, the MSB would have had trouble coordinating the relief work and alleviating the effects of the incident, as well as creating a satisfactory basis for collaboration.

4.4 Information coordination and communication

The disruption affected a large number of organisations and individual citizens. Being able to provide information about what has occurred and give advice and recommendations on an ongoing basis is a central function of emergency management for all public actors and affected organisations. It is of crucial importance to be able to coordinate information to the public for the purpose of providing a complete picture of impact, affected actors, necessary actions and progression of events.

In addition to the need to reach out to individual citizens and organisations, the mass media's **need for information must be** satisfied. The mass media is an important communication and information channel. Contacts with the mass media may, however, lead to additional speculation if there is not a clear communication strategy in place. Therefore, the mass media must be given access to quality information early on.

In the event of an IT incident, an additional problem is that the normal information and communication channels may have been impacted by the incident, i.e. websites, telecommunications, and e-mail may not be available.

³⁸ Utvärdering SAMÖ-KKÖ 2011 - kortversion. Publication number: MSB326 - October 2011, MSB.

In regards to the Tieto disruption, the affected organisations, which are the **company's customers**, have a great responsibility in terms of informing their users and other stakeholders themselves. The event shows that this responsibility is difficult for many actors to fully live up to. There are three main reasons for this:

- Tieto could not provide information on when the incident was expected to be rectified. This piece of information is the one that interested the affected organisations and their users the most.
- In many cases, the regular communication channels of the affected organisations, such as internal and external websites, as well as e-mail services, had gone down.
- Many of the affected organisations had not prepared any alternative communication channels.

Krisinformation.se conveys information from governmental agencies to other responsible parties regarding how to handle different emergencies – before, during and after they occur. The website is aimed at the general public and the media. Krisinformation.se is operated by the MSB and the content is drafted by joint government work groups from different fields. In connection with the disruption at Tieto, a discussion regarding how Krisinformation.se could work as an alternative website for Apoteket AB was held. This alternative was, however, deemed unsuitable since the website is only to serve as a platform for public information.

An increasing number of critical societal functions are operated by private actors. The purchaser may, however, still be a public organisation. The disruption at Tieto shows that there are several uncertainties surrounding the roles of different actors when it comes to communicating loss of services. The loss of function at the large logistics company affected, among others, a large number of operations in the Stockholm County Council. In such a situation, it can be difficult to know whether the company is to communicate with each section of operations or with the purchaser's organisation as a unit. Should communication be handled by the public purchaser or by the contracted private actor? Can a private executor gain access to the same communication channels as the purchaser and, thereby, be able to communicate on the same terms?

In this respect, it is very important to clarify that, even if operations are outsourced, the public purchaser is accountable to citizens. If a private organisation carrying out a public assignment is expected to communicate with citizens, this must be specified during the procurement process. Appropriate communication channels must also be established.

4.5 Emergency preparedness and contingency planning with a focus on information security

Emergency preparedness and contingency planning for long disruptions is a requirement for most organisations, but special needs arise when an

organisation outsources IT operations or uses cloud services for vital parts of the operation. In such cases, an agreement between the customer and the supplier is required in order to clarify the distribution of responsibility and the measures that are to be applied in the event of an unplanned disruption.

When an organisation outsources IT operations to a supplier or uses cloud services to a large extent, it is important to remember that responsibility for maintaining operations always remains with the outsourcing organisation. This means that the organisation must be prepared and have planned which measures to take in the event of a long disruption, where requirements on the supplier become a part of the internal planning.

Contingency planning must be based on a risk analysis and clear prioritisation from the management – a prioritisation that stipulates which aspects of the organisation are the most important to maintain. Based on this, requirements can then be placed on internal and external IT resources. Risk analyses are thus a necessary prerequisite for setting requirements.

Governmental agencies³⁹ are covered by the MSB's instructions on information security. In these regulations, which are based on the management system for information security, risk and vulnerability analyses, as well as risk management, are critical components. The management system is a central component of contingency planning.

In addition, the governmental agencies mentioned in the Emergency Management and Heightened Alert Ordinance (2006:942) have a special responsibility in terms of planning for measures that enable society to withstand strains of various sorts, from emergencies to heightened states of alert. The Government stresses the importance of this planning and of maintaining a comprehensive picture that covers the entire threat scale. Governmental agencies to which this regulation applies should, for instance within coordination areas, work on measures for emergency situations in peacetime and plan for measures during times of heightened state of alert.⁴⁰

A number of municipalities were affected by the disruption at Tieto. According to the Act on municipal and county council measures before and during extraordinary events in peacetime and periods of heightened alert (2006:544), municipalities are required to maintain emergency preparedness planning. However, the Act does not specifically cover IT incidents. On the other hand, the municipalities are bound by the MSB's instructions on risk and vulnerability analyses, which include requirements for each municipality and county council to assess their emergency preparedness capability. An indicator for the assessment is whether or not there is a plan for handling exceptional events. Considering that all organisations today are dependent on information management to maintain operations, it should be considered reasonable for the plan to include information on requirements for suppliers of IT operations and IT related services.

³⁹ The statute applies to governmental agencies under the rule of the Government, with the exception of the Government Offices, Government Committees and the Swedish Armed Forces.

⁴⁰ Bill 2011/12: 1 (Budget proposal for 2012), expenditure area 6

Customers that purchase various IT operations services are in general able to regulate availability requirements in their respective contracts, especially through standardised service level agreements provided by the suppliers. These agreements generally define the level of accepted disruption, and can therefore be seen as a description of the normal status. In addition, the agreements should include requirements for minimising the negative consequences of an emergency situation, as well as activities that are to be pursued during a restoration phase. There should be a requirement for contingency planning by the supplier and a commitment by the supplier to participate in exercises of the customer's plans. The requirements placed on the supplier assume a well-prepared plan by the customer, in order for processes to be maintained in the event of a disruption. The supplier should, however, be able to offer different levels of redundancy so that the customer can choose an acceptable risk level. This can be achieved, for example, by using the "dual sites" function, which provides geographically separated platforms that are connected, which means that information and services are replicated and accessible from more than one site.

Public actors, around 700 organisations, are able to use the Legal, Financial and Administrative **Service Agency's** framework agreements for IT operations and e-administration support services. The recent agreement includes an appendix regarding availability,⁴¹ which is missing from the framework agreement for IT operations. In both cases, the standard **"IT-företagens Allmänna Bestämmelser: IT-Drift version 2008"** applies. **This standard has an overall requirement for suppliers to help correct malfunctions that affect the service.**⁴² In addition, public customers can make sign agreements that include more explicit requirements for maintaining the service, as well as for contingency planning and redundancy. The Legal, Financial and Administrative Services Agency's view is that this possibility has not yet been used to a significant degree.

The picture is complicated further by the fact that a public organisation's requirement for contingency often must be transferred through several contract stages, such as when a county council procures services from a private health care provider, which in turn employs a large logistics supplier, which in turn procures IT operations services. It can be very difficult for the entity responsible for medical care (county council) to be certain that the requirements are upheld.

⁴¹ The Legal, Financial and Administrative Services Agency's framework agreements for e-administration services, Sections 3.14: "Service continuity and availability management. The supplier is to have a process for managing service continuity and availability. The requirements for service availability and continuity are to be identified with regard to the customers' business plans, service level agreements and risk assessments. The requirements are to include access rights and response times, as well as availability for the entire chain of system components. Availability and continuity plans for the service are to be developed and reviewed at least once per year in order to ensure that the requirements are met in accordance with the agreement under all conditions, from normal to prolonged or serious service disruptions. Availability is to be measured and registered. Unplanned unavailability is to be investigated and appropriate action shall be taken."

⁴² IT & Telecommunications companies, *Allmänna bestämmelser, IT-drift version 2008*, Section 15.1: "The supplier is to correct service problems caused by circumstances for which the supplier is responsible within the time specified in the Appendix on guaranteed service level, when applicable. Other errors are to be corrected at the speed required by the circumstances."

The impression after the disruption at Tieto is that the **actors'** contingency planning was of varying character. Some of those affected had relatively good planning in place where, for example, the logistics company could take advantage of the planning that was done for the influenza A(H1N1) pandemic, while other actors improvised. Apoteket AB could partially restore an older system and use supplementary manual routines, while other affected actors had only rudimentary planning in place for this type of an event. It is worth noting that several actors did not have backup routines for communicating with employees, the general public or customers, despite the fact that sound communication is crucial to managing an emergency.

Formal requirements placed on the supplier in regards to emergency preparedness or contingency planning have been observed to a small extent among the organisations affected by the disruption. The logistics company, for example, states that one of its customers, a large public actor, included requirements for emergency preparedness planning in the agreement, and Tieto had similar responsibilities towards other customers.

Tieto has verbally presented its contingency planning, which is primarily based on international standards for IT operations, and the company states that its planning worked out well considering the circumstances. An observation made by the company as a supplier is that customers with more comprehensive contingency planning and thus more advanced requirements on the supplier were affected less by the incident than other customers. For example, these customers had requirements for dual site solutions that provide better security in exchange for an increased cost.

Both Tieto and other suppliers have stated that in the event of an emergency, they make their own prioritisations based on what they consider to be critical societal functions, regardless of service level agreements and other agreements. These prioritisations have sometimes contradicted the supplier's own commercial interests. This means that customers with more extensive planning and comprehensive agreements with suppliers regarding availability still cannot be sure that they will be provided with the service stipulated by their contracts when it comes to information security. In other words, there is a strong element of unpredictability both for individual customers and in general since, in practice, the supplier decides how to prioritise customers.

The discussion on what is to be considered a critical societal function and the desire among actors in society to define these functions are not new. In the assessment of preparations for and management of the influenza A(H1N1) pandemic, the MSB and the National Board of Health and Welfare noted that the process for identifying and prioritising critical societal functions caused problems for the affected actors.⁴³ The concept of critical societal functions has, however, been clarified in the national strategy for the protection of critical societal functions, which the MSB presented in May, 2011.⁴⁴ Within the

43 *Influenza A(H1N1) 2009: Utvärdering av förberedelser och hantering av pandemin*. The Swedish Civil Contingencies Agency and the National Board of Health and Welfare.

44 *Ett fungerande samhälle i en föränderlig värld. Nationell strategi för skydd av samhällsviktig verksamhet*. Publication number: MSB266 - December 2011, MSB.

framework of the Styrel project, a number of criteria for identifying and prioritising critical societal functions have been established.⁴⁵

The MSB's summary assessment is that many affected organisations have shortcomings in their contingency planning and emergency preparedness for this type of incident.

4.6 Risk analyses with a focus on information security

A risk analysis is a prerequisite for outsourcing IT operations or procuring more extensive cloud services in a conscious manner.

Information security is to be treated in the risk and vulnerability analyses that public organisations are to carry out on a yearly basis in accordance with the MSB's instructions.⁴⁶ In addition, governmental agencies and other actors, such as municipalities and county councils that are comprised by the Security Protection Ordinance (1996:663) are obligated to review which operations are in need of security protection as regards national security and protection against terrorism. This may include information that is worthy of protection and resources for handling such information. An important part of this is the obligation to carry out a security analysis.

Furthermore, there are also requirements for risk and vulnerability analyses in the Personal Data Act (1998:204). The controller responsible for such records must carry out a risk and vulnerability analysis for the purpose of assessing the feasibility of engaging the service supplier for managing the records in question, which level of security is appropriate and which measures need to be taken. It is also worth noting that any organisation using external services for processing personal records is still responsible for such processing, even when it is carried out by a supplier or subcontractor.⁴⁷

Efforts to include information security in risk and vulnerability analyses are still at the developmental phase among many actors. In addition, it is also difficult for an individual actor to assess the degree to which the concentration of the IT operations area affects **the organisation's exposure to risk**.

A separate risk analysis should be carried out prior to all large procurements that can affect information security. An important part of this is the information classification that all organisations should apply in order to assess alternatives and to set security requirements.

During the analysis of the disruption at Tieto, it was observed that only a small number of actors had applied information classification or performed a risk

⁴⁵ Styrel is a nationwide planning system for prioritizing critical societal electricity users in the event of a predicted or sudden short-term power disruption. The Swedish Energy Agency is responsible for the implementation of Styrel planning. In 2011, planning was carried out in all of Sweden's municipalities, county councils and counties. As of 2012, a disconnect of electricity users in accordance with the plan is possible.

⁴⁶ MSBFS 2010:7 *föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser*, and MSBFS 2010:6 *föreskrifter om kommuners och landstings risk- och sårbarhetsanalyser*.

⁴⁷ Read more about cloud services and the Personal Data Act on the Swedish Data Inspection Board's website: <http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/>

analysis before their procurement and outsourcing of services. The MSB's assessment is that this obstructs well-functioning contingency planning, since the organisations have probably not conducted any in-depth analysis of their dependency on the outsourced resource.

4.7 Learning from IT incidents

During the acute phase of a major incident or emergency, the possibility to reflect is strongly limited. Therefore, in order to assess long-term effects, there is a need for feedback when normal conditions have been restored. Learning from accidents and emergencies is an important part of preventive and preparatory work and makes up an important basis for efforts related to emergency preparedness plans, risk and vulnerability analyses, collaboration, regulation, training, drills and more.

More than anything, the disruption has highlighted availability aspects. There is, however, reason to revisit how accuracy and traceability have been affected, and the extent to which information was lost. In addition, it is also probable that additional actors were affected indirectly by the incident.

An interesting aspect that is particularly important to take into consideration is the financial impact, which is most likely very extensive. This is an important factor to consider in future risk analyses at all levels of responsibility and within all sectors of society.

For the MSB's future work within the field of information security, as well as from a wider emergency management perspective, it is important to learn from the experiences of the actors affected by the incident and how they experienced management of the incident. Doing so means the quality of the preventative work can be assured and useful lessons can be learned about supporting and coordinating efforts at the acute stage (preparatory).

5. Final reflections and further work

5.1 Final reflections

Sweden's emergency management relies on collaboration. All actors must be able to act together and collaborate on decision-making and operations in the event of an emergency. The responsibility principle, the proximity principle and the equality principle are important points of departure for Sweden's emergency preparedness. An emergency is initially handled in its immediate vicinity, while resources at the regional and national levels are available if the incident becomes too extensive to be handled on a local level. The municipalities' operations form the basis for basically all emergency management. During an emergency, the county administrative board is to support the municipality's collaboration with other governmental agencies, municipalities and other actors, as part of the county administrative board's overall geographic responsibility at the regional level.

The increased concentration of IT operations and other IT related services, such as cloud computing, create new opportunities and also societal risks. This change in forms of delivery may be a way to both increase quality and reduce business costs. The incident shows that a disruption at a large IT operations supplier can affect an entire society and that the impact can be considerable. Modern society continues to increase in sedentariness when IT systems become unavailable.

In the event of IT incidents, warnings come at short-notice or not at all, the pace is rapid and the incident is usually geographically independent. In order to prevent and handle major IT incidents, an increased capability of all actors in society at all levels of responsibility and in all sectors is required. The disruption at Tieto shows that the actors in the emergency management system need to develop their capability as regards situation status reports and comprehensive impact and handling assessments. Several of the actors do not have sufficient knowledge of their own dependencies, or about their need for cooperation. In many cases, internal emergency preparedness could also be developed.

It is important to further create prerequisites that allow for the use of society's common resources in order to prevent and handle major IT incidents. Knowledge of the competencies and roles found in the public and private sectors needs to be increased. Involved actors need be aware of their counterparts' roles and of what information other actors need and can offer.

5.2 Further work

Strengthened preventive initiatives for information security throughout society

Preventive information security work needs to be developed on all levels of responsibility and within all sectors, and must be further coordinated in order to prevent and manage major IT incidents in society. In order to increase society's information security, increased collaboration between public and private actors is required.

This work should continue in line with the strategy for **society's** information security.⁴⁸ The national action plan, which is being drafted in collaboration with governmental agencies in the Cooperative Group for Information Security (SAMFI), will provide additional clarification.⁴⁹

The disruption shows that actors with sector responsibilities, such as governmental agencies, county administrative boards, county councils and municipalities need to improve their capability to prevent and handle IT related emergencies.

Procurement as a tool for better security

There is a lot of potential in public procurement, and all actors need to further develop their competency in using procurement as a means to control their information security.

Agreements can also be formulated to include rules that support **society's** emergency management, such as requirements for reporting incidents and how suppliers are to contribute in the event of serious disruptions. This type of control is considered appropriate since public organisations are increasingly acting as buyers of various services. In addition, contract terms can also be passed on to subcontractors.

The overall procurement awarded by virtue of the Swedish Administrative Services Agency is an important tool for increasing information security in public administration.

Special focus on risk analysis and contingency planning

The disruption at Tieto shows that there are shortcomings in the contingency planning and emergency preparedness among several of the affected organisations. Systematic work related to information classification and risk analyses is a prerequisite for all work involving information security.

⁴⁸ *Strategy for information security in Sweden 2010-2015*. Publication number: MSB 243, MSB.

(<https://www.msb.se/RibData/Filer/pdf/25940.PDF>).

⁴⁹ The Cooperative Group for Information Security (SAMFI) consists of six governmental agencies with specific tasks within the field of information security. SAMFI will exchange information and support the relevant authorities' tasks within the field. The following governmental agencies are members of SAMFI: the Swedish Defence Materiel Administration (FMV), the National Defence Radio Establishment (FRA), the Swedish Armed Forces (FM), the Swedish Civil Contingencies Agency (MSB), the Swedish Post and Telecom Authority (PTS) and the National Police Board (RPS), which is represented by the Swedish Security Service (Säpo) and the National Bureau of Investigation (RKP).

Since the information management of critical societal actors is increasingly being built on technologically and organisationally integrated solutions, risk analyses and contingency planning are becoming complex. Risk analyses – information classification in particular – are important tools for procurement. From this perspective, collaboration is important since the public sector's procurements can more or less be performed through the Legal, Financial and Administrative Services Agency's framework agreements. Risk analyses can thus be a driving factor for overall improved information security.

It is important to develop support that allows organisations with limited resources to carry out risk analyses and information classification, as well as contingency planning.

Contingency plans and other frameworks for IT incident management need be practiced and updated on a regular basis.

National and regional situation status reports on information security

The increased concentration of IT operations and other IT related services means that a large number of actors might be affected simultaneously by an incident, and that the consequences for society may be major. This imposes increased requirements for collaboration and coordination.

Cooperation and coordination of a major IT incident assume that there are relevant and current situation status reports at local, regional, sector and national levels. The disruption at Tieto shows that the affected actors need to develop processes for gathering and sharing information. This should also include being able to communicate information to citizens, and it assumes that the information is coordinated.

The MSB intends to continue its efforts to develop a national situation status report on information security in collaboration with affected actors in society. A basic premise for this work is the National Cybersecurity Coordination Function (NOS). Special focus will be given to the necessity of quickly being able to obtain situation awareness from different actors throughout society, such as governmental agencies and county councils with sector responsibilities. An important question that must be answered is how situational information is to be collected from private actors in a way that does not risk their business integrity or need for confidentiality.

Another important aspect of creating a national situation status report on information security is a system for mandatory IT incident reporting for governmental agencies.⁵⁰ Considering the disruption at Tieto, the MSB believes that it should be considered whether other public actors, such as municipalities, should also be covered by this mandatory reporting of IT incidents.

⁵⁰ For more information, see the MSB's response to the government assignment regarding mandatory IT incident reporting (assignment presentation 01/03/2011, journal number 2010-6307).

In Bill 2011/12: 1 (Expenditure area 6) the Government writes that the MSB will be tasked with conducting an in-depth analysis of mandatory IT incident reporting for governmental agencies.

Appendix 1: Request in accordance with the Emergency Management and Heightened Alert Ordinance (2006:942)



Myndigheten för
sambhällsskydd
och beredskap

Hemställan

Datum
2011-12-06

Diariernr
2011-6477

Ert datum

Er referens

1 (3)

Avdelningen för samordning och insats
Tjänsteman i beredskap

Enligt sändlista

Hemställan angående information om driftstörningar orsakade av större hårdvarufel hos Tieto

Under den senaste veckan har ett antal samhällsaktörer som Apoteket AB, Apotekens Service AB, Stockholms stad och Bilprovningsdrabbats av omfattande driftstörningar orsakade av problem hos deras tjänsteleverantör Tieto. På grund av de avtalsmässiga förhållandena kan Tieto inte avslöja vilka kunder som har blivit drabbade.

Myndigheten för samhällsskydd och beredskap (MSB) kommer att göra en utredning angående vad som hänt hos Tieto. Utredningen kommer att ske med utgångspunkt från MSB:s uppdrag att analysera hot och risker i samhället som kan anses vara särskilt allvariga. En viktig del i detta är att förstå de konsekvenser som incidenten lett till samt att ta fram förslag på åtgärder som kan leda till ett förbättrat skydd för såväl samhället som för enskilda aktörer.

Myndigheten för samhällsskydd och beredskap (MSB) begär i enlighet med 15 § förordningen (2006:942) om krisberedskap och höjd beredskap att myndigheterna enligt sändlistan lämna en lägesbedömning enligt nedanstående punkter. Försvarmakten lämnar uppgifter efter eget beslut.

1. Är några aktörer inom ert ansvarsområde drabbade av ovanstående händelse?
Om svaret är ja på fråga 1 besvaras även följande frågor:
2. Vilka aktörer har blivit drabbade och på vilket sätt?
3. På vilket sätt har ni fått information om det inträffade hos dessa aktörer?
4. Kan ni bedöma om aktörernas verksamhet i nuläget fungerar normalt eller finns det kvardröjande negativa effekter?

Lägesbedömningen ska lämnas till MSB senast kl 13.00 den 14 december på adressen:

MSB Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Besöksadress:
Stockholm: Kungsgatan 53
Karlstad: Norra Klaragatan 18
Sandö: Sandövägen 7
Revinge: Revingeby

Telefon: 0771-240 240
Fax: 010-240 56 00
Kryfax 010-240 43 63

registrator@msb.se
www.msb.se

Org nr.
202100-5984

Myndigheten för
samhällsskydd och beredskap

Hemställan

Datum
2011-12-06

Diarienum
2011-6477

2 (3)

Fia Ewald
Avd. för risk- och sårbarhetsreducerande arbete
Enheten för samhällets informationssäkerhet
fia.ewald@msb.se

Postadress:
651 81
KARLSTAD

Om de svar ni lämnar innehåller känslig information använd kryfax 010-240 43 63. Informationen kommer att skyddas i enlighet med Offentlighets- och sekretesslagen (2009:400).

SÄNDLISTA

Datainspektionen datainspektionen@datainspektionen.se
Energimyndigheten registrator@energimyndigheten.se
Finansinspektionen finansinspektionen@fi.se
Kustbevakningen registrator@kustbevakningen.se
Livsmedelsverket livsmedelsverket@slv.se
Läkemedelsverket registrator@mpa.se
Länsstyrelsen i Blekinge blekinge@lansstyrelsen.se
Länsstyrelsen i Dalarna dalarna@lansstyrelsen.se
Länsstyrelsen i Gävleborg gavleborg@lansstyrelsen.se
Länsstyrelsen i Gotlands län gotland@lansstyrelsen.se
Länsstyrelsen i Halland halland@lansstyrelsen.se
Länsstyrelsen i Jämtlands län jamtland@lansstyrelsen.se
Länsstyrelsen i Jönköpings län jonkoping@lansstyrelsen.se
Länsstyrelsen i Kalmar län kalmar@lansstyrelsen.se
Länsstyrelsen i Kronobergs län kronoberg@lansstyrelsen.se
Länsstyrelsen i Norrbottens län norrboten@lansstyrelsen.se
Länsstyrelsen i Skåne skane@lansstyrelsen.se
Länsstyrelsen i Stockholms län stockholm@lansstyrelsen.se
Länsstyrelsen i Södermanland sodermanland@lansstyrelsen.se
Länsstyrelsen i Uppsala län [uppsala@lansstyrelsen.se](mailto: uppsala@lansstyrelsen.se)
Länsstyrelsen i Värmlands län varmland@lansstyrelsen.se
Länsstyrelsen i Västerbotten vasterbotten@lansstyrelsen.se
Länsstyrelsen i Västernorrlands län vasternorrland@lansstyrelsen.se
Länsstyrelsen i Västmanland vastmanland@lansstyrelsen.se
Länsstyrelsen i Västra Götalands län vastragotaland@lansstyrelsen.se
Länsstyrelsen i Örebro län orebro@lansstyrelsen.se
Länsstyrelsen i Östergötland ostergotland@lansstyrelsen.se
Post- och telestyrelsen pts@pts.se
Rikspolisstyrelsen rikspolisstyrelsen@polisen.se
SMHI smhi@smhi.se

Myndigheten för
samhällsskydd och beredskap

Hemställan

Datum
2011-12-06

Diarienum
2011-6477

3 (3)

Socialstyrelsen socialstyrelsen@socialstyrelsen.se
Strålsäkerhetsmyndigheten registrator@ssm.se
Svenska Kraftnät svenska.kraftnat@svk.se
Trafikverket registrator@trafikverket.se
Transportstyrelsen registrator@transportstyrelsen.se
Tullverket tullverket@tullverket.se
Försvarsmakten (omfattas ej av 15 §, eget beslut om rapportering)
exp-hkv@mil.se

För kännedom:

Fö/SSK

Appendix 2: Privacy declaration



Myndigheten för
sambhällsskydd
och beredskap

Verksamhetsstöd
Rättssenheten
Torkel Schlegel
010-2405069
torkel.schlegel@msb.se

Datum
2012-01-09
Ert datum

Darienum
Er referens

1 (3)

Tieto Sweden AB
Katarina Aurell
Fjärde bassängvägen 15
115 83 Stockholm

Förklaring om sekretess i samband med MSBs utredningar m.m.

Inledning

Myndigheten för samhällsskydd och beredskap (MSB) har genom sin instruktion ett generellt uppdrag att samverka med näringslivet för att identifiera och analysera sådana sårbarheter, hot och risker i samhället som kan anses vara särskilt allvarliga. MSB ska värdera, sammanställa och rapportera resultatet av sådant arbete till regeringen.

MSB har nu inlett en samverkan med Tieto Sweden AB (Tieto) för att utreda en under november 2011 inträffad IT-incident hos Tieto.

För MSBs verksamhet gäller offentlighetsprincipen som innebär att de handlingar som förvaras på myndigheten och som inkommer eller upprättas på myndigheten är allmänna handlingar. Dessa ska som huvudregel vara offentliga och lämnas ut på begäran. Finns däremot en tillämplig sekretessbestämmelse får myndigheten inte lämna ut sekretessbelagda uppgifter i handlingen. Sekretessbestämmelsen innebär också en tystnadsplikt för myndighetens medarbetare gällande de uppgifter som träffas av sekretessbestämmelsen. Brott mot tystnadsplikten är straffsanktionerat enligt 20 kap. 3 § Brottsbalken.

Frågan om sekretess för en uppgift prövas inte i förväg utan först när uppgiften ska lämnas ut. Det är MSB som självständigt prövar frågan och MSBs beslut att neka utlämnande kan överklagas till Kammarrätt.

Om MSB genom sin samverkan med näringslivet genomför en utredning för att identifiera och analysera allvarliga sårbarheter, hot och risker i samhället finns det tillämpliga sekretessbestämmelser varav den mest relevanta för nu aktuella utredningsverksamhet beskrivs nedan.

MSB Myndigheten för samhällsskydd och beredskap

MSB-1.4

Postadress: 651 81 Karlstad	Besöksadress: Stockholm: Kungsgatan 53 Karlstad: Norra Klaragatan 18 Sandö: Sandövägen 7 Revinge: Revingeby	Telefon: 0771-240 240 Fax: 010-240 56 00 registrator@msb.se www.msb.se	Org nr. 202100-5984
---------------------------------------	--	---	------------------------

**Myndigheten för
samhällsskydd och beredskap**Datum
2012-01-09

Diarienum

2 (3)

Tillämpliga regler

Genom offentlighets- och sekretesslagen (OSL) 30 kap. 23 §, offentlighets- och sekretessförordningen 9 § och förordningens bilaga punkt 13 följer att när MSB utreder frågor med avseende på näringslivet gäller sekretess för uppgifter om affärs- eller driftförhållanden, uppfinningar eller forskningsresultat om det kan antas att näringsidkaren lider skada om uppgifterna röjs.

Om MSB t.ex. samverkar med näringslivet för att utreda vilken samhällspåverkan ett inträffat fel i ett IT-system kan ha, är denna sekretessbestämmelse tillämplig. Sekretessen gäller inte alla uppgifter som myndigheten kan tänkas ta del av men borde täcka det som är väsentligast för näringsidkarna i och med skaderekvisitet.

Enligt samma lagrum råder en absolut sekretess för uppgifter som rör den som trätt i affärsförbindelse eller liknande (t.ex. Tietos kunder m.fl.) med den näringsidkare som myndigheten samverkar med.

Även andra sekretessbestämmelser kan vara tillämpliga beroende på vad för slags uppgifter det gäller. Enligt 18:8 OSL gäller sekretess för uppgifter om säkerhets- eller bevakningsåtgärder om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärderna avser telekommunikation eller system för automatiserad behandling av information. Denna sekretess kan t.ex. användas för uppgifter om "brandväggar" och liknande.

Meddelarfrihet

Meddelarfrihet innebär i korthet att den enskilde myndighetsmedarbetaren kan lämna muntliga uppgifter till media. Meddelarfriheten följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Meddelarfriheten bryter sekretess enligt 30:23 OSL för uppgifter som rör den näringsidkare myndigheten samverkar med, dock inte för denne näringsidkares affärspartners m.fl.. Se 30:30 OSL. Meddelarfrihet gäller inte heller för uppgifter som omfattas av sekretess enligt 18:8 OSL.

Förfogande över material

Om handlingar lämnas över till myndigheten, sk inkomna handlingar, förlorar näringsidkaren rådigheten över dessa och dess information. Näringsidkaren kan inte begära att få tillbaka dessa eller att materialet ska förstöras. Det kan i och för sig finnas upphovsrätt till materialet men det begränsar bara vad myndigheten kan utnyttja materialet till, inte att myndigheten får och ska behålla det.

Samverkan mellan MSB och Tieto

Gällande rätt

MSB kommer att hantera all information, skriftlig eller muntlig, i enlighet med gällande rätt och enligt de skyldigheter gällande rätt ålägger myndigheten. MSB kommer också att göra vad som åligger myndigheten för att informera myndighetens medarbetare vilka skyldigheter de har enligt gällande rätt.

Dokumentation och skriftligt material

MSB kommer under samverkan med Tieto inte att begära in någon dokumentation eller skriftligt material. MSB kommer endast att ta emot sådant material om det är Tietos avsikt att MSB ska ta emot materialet.

Tietos företagshemliga material

MSB är införstådda med att Tieto anser att allt material och all information som MSB kan komma att få ta del av kan vara sådan att det skadar bolaget eller bolagets affärspartners om det offentliggörs.

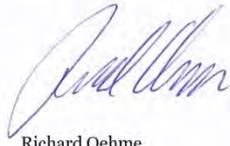
Yttrande i samband med skadeprövning

Om det blir aktuellt att pröva en fråga om att lämna ut uppgifter eller allmänna handlingar som kan omfattas av sekretess och där uppgifterna eller handlingarna på något sätt härrör från Tietos verksamhet och kommit MSB tillhanda i samband med samverkan för utredning om nu aktuella IT-incident kommer MSB att ge Tieto tillfälle att yttra sig om på vilket sätt ett offentliggörande kan vålla Tieto eller dess affärspartners skada.

Vid en begäran om utlämnande av allmän handling är MSB skyldig att skyndsamt pröva frågan. Tietos måste därför också hantera sitt yttrande skyndsamt.

Beredning

Denna avsiktsförklaring har gjorts av Richard Oehme, chef för enheten för samhällets informationssäkerhet. Torkel Schlegel, chef för Rättsenheten har varit föredragande.



Richard Oehme



Torkel Schlegel

