Dependability of IT Systems in Municipal Emergency Management

Kim Weyns
Lund University
kim.weyns@cs.lth.se

Martin Höst
Lund University
martin.host@cs.lth.se

ABSTRACT

In recent years governmental actors have become more and more dependent on IT systems for their responsibilities in a crisis situation. To avoid unexpected problems with the dependability of IT systems in the aftermath of a crisis it is important that such risks are identified and that measures can be taken to reduce the dependence on systems that could be unreliable.

This paper describes two case studies exploring how Swedish municipalities incorporate IT systems in their emergency planning. The study focuses especially on how different actors within a municipality cooperate to analyse the risks of depending on IT systems in critical situations. The study shows that today there is much room for improvement, especially in the communication between IT personnel and emergency managers.

Finally, this paper describes the requirements for a process improvement framework that can assist governmental actors in analysing and improving their dependency on IT systems in emergency management.

Keywords

Emergency management, IT management, dependability, risk and vulnerability analysis.

INTRODUCTION

In recent years governmental actors have come to depend more on IT systems for all their everyday tasks. For communication, municipalities depend on landline telephone networks, mobile phone networks, webservers, email servers, etc. Other important systems are used for patient administration in health care and social care, school administration or city planning.

Just as for their everyday tasks, governmental actors now depend on all kinds of IT systems for their responsibilities in crisis situations. These systems include not only specially built systems for emergency situations but also the everyday systems described above. The latter category of systems is of special interest, because under normal conditions an occasional unavailability of these IT systems might be acceptable, but during crisis relief, when time is a critical factor, any unexpected unavailability can have disastrous consequences. Therefore, it is important that these IT systems are an integral part of all major risk and vulnerability analyses conducted.

Based on two case studies and a survey, this article presents how Swedish municipalities, with an important active role in crisis relief, include IT systems in their emergency planning and vulnerability analyses. This paper first focuses on the main problems experienced by practitioners today and then shortly describes the requirements for a process improvement framework that could help organisations to improve the way they deal with IT dependability in emergency management.

BACKGROUND

Dependability

For all software engineering concepts concerning dependability we will follow the definitions from Avizienis et al. (Avizienis, Laprie, Randell and Landwehr, 2004). This means that dependability takes into account all more specific aspects such as reliability, availability, safety and security and corresponds best to the intuitive notion of how much a system can safely be depended upon by its users.

Emergency Management in Sweden

Swedish emergency management (KBM, 2005) is mainly based on the ‘principle of responsibility’, which means that in emergency conditions the responsibilities for everyday matters should still lie with those

governmental actors that are also responsible for these matters in normal conditions. Through the principles of proximity and geographic area responsibility, emergency management is in the first place a responsibility of the local governments. Practically, this means that municipalities are the central actor in crisis relief. Only with crises that affect many municipalities the regional governments are directly involved in an operative role.

For their emergency planning, Swedish municipalities receive support from the Swedish Emergency Management Agency (SEMA). SEMA assists the municipalities by educating them about emergency planning and by providing guidelines. Unlike the emergency management agencies in many other countries, SEMA does not have an operative role in crisis relief. An extensive description of Swedish emergency planning at the municipal level can be found in the referenced articles (Hallin, Nilsson and Olofsson, 2004).

RELATED WORK

Internationally, more and more research is being done on special systems that can be used in crisis relief. The near future will almost certainly see a quick rise in the number of IT systems used in crisis situations. So far most of these systems are only considered as an extra tool in the aftermath of a crisis, but as these tools become more common, emergency responders will also become more critically dependent on them. Therefore it will become even more important to fully integrate these IT systems into emergency management and include them in the vulnerability analyses that are conducted.

In the private sector, a lot of research has been done on improving the cooperation between an organisation's IT department and the rest of the organisation. For example Luftman (Luftman, 2003) describes a maturity model for improving this cooperation, which is similar to the process improvement framework we propose in section 7 of this paper. The area of IT management that is most relevant to this research is often called business continuity management, which is concerned with maintaining a reasonable level of service during emergency situations. However, an important difference is that, unlike private actors, governmental actors with emergency relief responsibilities have to attain an even higher than normal level of service during emergency situations, which poses special requirements on their IT management. Conditions during emergency relief operations are often very different from normal conditions. Traditional IT management frameworks often have a strong focus on business aspects and neglect the special needs of organisations with an active role in crisis relief. Many of the problems discussed in this paper can also be found in regular IT management, but because IT dependability is especially critical during emergency situations and because the focus of IT management is mostly limited to normal conditions, the problems with IT dependability management in emergency conditions deserve special attention.

To help Swedish governmental actors with the dependability of their IT systems, SEMA published BITS, the Basic Level for IT Security handbook (SEMA, 2003). BITS is meant to give Swedish authorities a practical overview of the main administrative measures that can be taken to achieve a minimum level of IT dependability. BITS is based on international standards such as ISO-IEC 17799 (International Organization for Standardization, 2005), but BITS is much more suited for small public actors. BITS is also accompanied by BITS Plus, a web based planning tool that can be used to coordinate the work with the BITS standard. The main disadvantage with using BITS for achieving a higher dependability is that it focuses mainly on security and a lot less on reliability and safety.

RESEARCH METHODOLOGY

The research in this paper combines results from two different sources: data collected from case studies at two Swedish municipalities and the data of a survey conducted by SEMA.

Case Studies at Two Swedish Municipalities

The main part of this research was conducted in two case studies at two different Swedish municipalities. These municipalities were selected because they had shown an interest in the topic of IT systems in emergency management in previous contacts with SEMA or with other members of our research project.

Municipality A is a large Swedish municipality consisting of a major Swedish city and the surrounding urban areas with close to 125,000 inhabitants and 7500 direct employees. Municipality B on the other hand is a small municipality consisting of two suburbs of a large Swedish city. Municipality A has 6 times more inhabitants, and also from a hazard perspective there are large differences. Municipality A houses a lot of industry and is an important national hub for the transport of dangerous goods. During the last years the municipality has gone through some major emergency situations of different types. Municipality B has a much lower risk profile and has not experienced any major emergency situations in the last 15 years.

To understand how these municipalities assess the dependability of their IT systems in emergency situations, a series of interviews were conducted with emergency managers and IT personnel at both municipalities. Further a number of documents concerning IT strategies, organisational structures and vulnerability analysis were also collected and studied.

For the analysis, all interviews were recorded and transcribed in full. During the transcription they were also translated from Swedish to English. Then, two authors went through all the transcribed text independently and coded (Robson, 2002) all excerpts according to the following categories: division of responsibilities, internal communication, service level agreements, risk analysis and practical examples of problems. Afterwards their lists were merged and the excerpts in every category and subcategory were analysed. Since the interviews often returned to the same topic, and because different people in the same organisation were interviewed, triangulation was used to check the consistency of the interviewees' answers. For the analysis both within and across the two municipalities the technique of explanation building (Yin, 2003) was used.

Survey by SEMA

In May 2005, SEMA conducted a survey among 368 IT security managers at all Swedish municipalities, regional governments and different public authorities. A first analysis of the 230 answers to the survey they received was published shortly afterwards (Kalmelid and Gustavsson, 2005).

The goal of the survey was to assess the capabilities of different governmental actors in the field of IT security. Within IT security the survey focused mostly on the methods and standards used and how SEMA's support towards the governmental actors could be improved. The respondents were also asked to make an assessment of the maturity of their organisation and different members of their organisation in IT security.

For our study, the answers to the survey's open questions were analysed in a similar way as the interviews in the case studies.

FINDINGS

This section contains the main findings from the case studies and the survey. Each of the next sections discusses the conclusions that can be drawn from the excerpts that were coded in to the corresponding categories listed above.

Division of responsibilities

In both municipalities that participated in the study there is a central IT unit responsible for the maintenance of the IT systems. The final responsibility for most of the systems lies with specific departments that are the main users of the system. This responsibility means they decide about the acquisition, the updates and the evaluation of the systems. This division of responsibilities is logical, but also has a number of problems.

A first problem lies in the evaluation of the dependability of the systems. Since the IT department is responsible for the maintenance they are contacted in case of any problems, but it is not their responsibility to collect failure statistics, as expressed in Quote 1. The system responsible is often not even notified of all the problems, and can not get a full picture of the dependability of the system. In municipality A, the IT department has a help desk that coordinates the maintenance work of the IT department. In municipality B, users contact one of the employees of the IT department directly on their mobile phone, making it even harder to collect failure statistics. Further, concerning the service that is outsourced to external suppliers, some failures are reported directly to the supplier, while others are reported to the supplier through the IT department.

We don't do any organised data collection now, we just try to solve the problems that come up.

Quote 1. IT Technician, Municipality B

A second problem is that in this organisational structure the separate departments, and in particular the emergency managers, do not have any own technical personnel that can advice them on the technical details that are involved in the administration of the IT systems. This can lead to responsibilities implicitly being shifted to the IT department, just because the different departments do not immediately know how to deal with them. This is for example complained about in the survey as can be seen in Quote 2.

The IT personnel should get better at defining the limits of their area of responsibility to make sure that the

responsibility is where it should be. This is necessary to avoid that the focus lies with the technology instead of the processes. We are not good enough at explaining to the different departments that there are some parts for which they must take responsibility. Today the IT department must always take responsibility for IT matters for which no-one else takes responsibility. This is not good.

Quote 2. Survey answer to the question: "What do you think the IT personnel could get better at concerning IT dependability?"

In municipality B, IT safety is a special responsibility of one of the emergency managers at the municipality. The advantage of this role is that he can lift these safety issues immediately to the highest levels in the municipality. In practice, a problem with this approach is that the IT department feels relieved of all safety responsibilities although their expertise is indispensable for evaluating this safety.

5.2 Internal Communication

An often recurring complaint, in the case studies and the survey, is a lack of real understanding between the IT department and the users, including emergency managers. Users complain that the IT personnel does not understand what they expect of their systems, as for example in Quote 3. The IT personnel on the other hand complains that the users do not understand the risks involved with IT systems, especially concerning security.

We have generators and we can provide backup power to our IT systems for a long time. Assuring the quality of our IT systems is more difficult. We have discussed this a lot, also with our IT technicians, but they often focus on the wrong things.

Quote 3. Emergency Manager, Municipality B

This lack of understanding is a consequence of the communication problems between both parties. Both municipalities under study lacked a forum where the IT department, the users and safety managers could discuss important strategic IT issues together. In the worst case the only communication occurs when a failure of a software system occurs and the IT department has to be notified to fix the problem.

Because of communication problems, many decisions about updates to the systems are made unilaterally and sometimes the other parties are not even notified in advance of the update. Of course, this also means that the risks of these changes cannot be analysed in detail, especially concerning specialised emergency scenarios unknown to the IT department.

Another common complaint about the communication between emergency managers and the IT department is that the communication from the IT department is too technical. Outside the IT department there is not enough technical knowledge to understand the technical details of the system, while the IT department does not manage to communicate their message without resorting to technical details. This adds to the frustration of both parties, and results in the IT department not being consulted as often as necessary for important decisions.

5.3 Service Level Agreements

Both municipalities in the study have some service level agreements, SLAs, with their external suppliers but have no service level agreements at all with their own IT department. Some written communication by which users and the IT department discuss the level of service, would offer clear advantages to both parties. For example in municipality B, the IT department tries to always have some IT personnel reachable to provide service, even in weekends and at night in case there is a need for urgent IT support for critical systems. This level of service is available because the IT department considers it reasonable, but is not explicitly specified anywhere as a guaranteed service. This illustrates again that the IT support is planned without consideration for emergency conditions.

The main advantage of SLAs for the users is that they know what to expect, and what not to expect, from their IT systems. This way they can avoid both depending on unreliable systems and investing in unnecessary backup

solutions for sufficiently reliable systems. This problem is expressed in Quote 4 from a project manager at municipality A.

> *If the IT department can explicitly state that they can not give us any guarantees, we can justify investing some extra millions ourselves to secure our systems. But without any defined service levels, we have no arguments to justify this cost here.*

Quote 4. Project Manager, Municipality A

Even the service level agreements with external suppliers are often not well planned and not adapted to the level of quality actually demanded by the users of the systems. For example at municipality B, the maintenance contract with their supplier of routers guaranteed on-site service within 8 hours. This number was agreed upon many years ago, and nobody recalls exactly why it once was set at 8 hours. The importance of the internal network for the daily operations at the municipality has definitely increased drastically since this decision was taken. This example shows there are no routines in place to regularly re-evaluate important service level agreements.

Service level agreements are closely connected to measurements. The writing of service level agreements forces an organisation to think about how the quality of its IT systems can be measured. Just as both municipalities lack service level agreement for most of their systems, they also lack the possibility to measure the quality of their IT systems. Access to such measurements would give them a possibility to concentrate their resources better to improve the weakest links in their critical systems.

5.4 Risk Analysis

Although IT systems can play an important role in the aftermath of a crisis, they are seldom included in the emergency plans and risk analyses that are conducted. Emergency managers would like to include these systems, but they do not manage to do so because of problems in cooperating with the IT department. In municipality A, the emergency management of the social care department is planned in such a way that, if necessary, the department can function completely independent of IT systems. This means, for example, that all critical information is printed out on a very regular basis and communication plans are ready that do not rely on modern technology. As the project manager explained, this is a safe solution, since it means they are prepared for a complete failure of all IT systems, but it is also a serious overhead cost that is only necessary because they do not manage to analyse the risks of depending on their IT systems. If they would manage to include the IT systems in their risk analyses, they would be able to evaluate which systems are reliable enough to depend upon in different emergency situations, and they could prioritise their resources by focussing on the least reliable and most critical systems. Because the IT systems are not part of the emergency plans, they can also not be used as efficiently in a crisis if they turn out to be reliable after all.

In municipality B, a crisis central was installed with the help of SEMA and a number of external consultants. Although IT systems are a critical component of the equipment there, the IT department was not involved in the development of this room. The IT department also maintains the systems in this room, but they are not involved in any strategic planning of how the systems in this room should be updated or replaced.

When the IT department is not involved in emergency planning, as expressed in Quote 5, they are also not aware of which systems are critical during different crisis situations and they can not correctly prioritise their maintenance work without receiving specific instructions during a crisis. IT systems are also seldom involved in emergency exercises. Useful lessons for emergency management could also be learned from exercises such as regularly trying to restore a system from backup, or measuring the behaviour of the network when one or more routers are disabled.

> *We are not involved in making emergency plans. It's not something we think about. And I don't know what the rules are for prioritised service in an emergency. Nobody told me whether one computer is more important than another.*

Quote 5. IT Technician, Municipality B

5.5 Common Problems

A first major problem that was observed at both the municipalities was the problem with defining who is responsible for evaluating the dependability of the IT systems in crisis situations. This task requires the cooperation between the emergency managers, the IT department and the department owning the system. In practice, because of the communication problems discussed before, this can lead to this issue being overlooked. Especially if the IT department is not involved in the strategical discussions about the IT systems, they limit themselves to the daily maintenance of the systems and only perform technical long-term improvements when explicitly asked.

A second recurring problem is the lack of good supporting tools or standards. BITS (SEMA, 2003), used by 75% of the municipalities that answered the survey, is more focused on security than reliability, and the focus is therefore more on the systems as separate units, and not on how the systems fit in to the overall activities of the municipality, as illustrated by Quote 6. For this reason, BITS is not ideal for a complete dependability analysis, and might even lead to some aspects being forgotten when it is not complemented with other risk analysis methods.

The main disadvantage of BITS is that it uses an object-oriented model for IT dependability, instead of a process-oriented model. This means it considers IT systems as isolated objects, instead of starting from the information processes that are provided or supported by the system.

Quote 6. Survey answer to the question: "What do you think could be improved about BITS?"

A third problem we observed lies in the emergency managers' limited understanding of the dependability issues of IT systems. When they want to conduct a risk analysis of the IT systems they need this technical knowledge to be able to understand all the threats to the reliability of the system, their probability and possible consequences. Often it is assumed that the IT systems can be depended upon in a crisis, even if there is no evidence of their reliability.

Finally, a typical problem with IT systems is their fast evolution. New IT systems are installed every year and updates are done even more regularly. Adding new functionality to old systems changes both the reliability of the system and the dependence on the system. Often municipalities do not manage to keep their risk analyses updated to reflect the latest functionality of the IT systems. This is especially important since the dependence on the IT systems is increasing continuously. At first, after a new system has been installed, the system is usually only considered an extra asset that could be useful in a crisis situation, even if it not critically necessary because the old alternatives are still available. At this time the dependability of the system is not critical, but when the users get more used to having the new system around, the alternative systems are neglected and the new systems can become more and more critical. When these changes occur gradually, they are sometimes only noticed too late and systems can become critical without their dependability ever having been seriously evaluated.

6 VALIDITY DISCUSSION

A first threat to the validity in this study is the possibility of researcher bias. All the interviews were conducted by the same researchers and the conclusions from the first interviews were used to steer the later ones. To minimise the effect of researcher bias, the interviews were conducted with two researchers present and extra care was given to let the interviewees tell their own story, without guiding their answers. In the analysis of the interviews the possibility of researcher bias was constantly taken into account when building explanations.

A threat to the construct validity that is often present when data is collected through interviews is the possibility that the participants are focusing too much on their own side of the story and give a distorted view of reality. Through the use of triangulation, by interviewing different people at the same municipality and by asking different questions concerning the same topic, the effect of this can be reduced. Overall, our impression was that the interviewees were not afraid at all to talk about problems they were experiencing or had experienced in the past.

Further, when considering the external validity of this study, it is important to reflect on how far the results can be generalized. The case studies studied only two municipalities, but there is good reason to assume that the problems identified in this study are not unique to just these two Swedish municipalities. Because many of the conclusions were very similar for both municipalities, and because they are also supported by the survey which was answered by a majority of the Swedish governmental actors, we believe that it is likely that similar problems can be found in many Swedish governmental organisations with an active role in emergency management. More research is necessary to determine how factors like the size of the governmental actor influence the conclusions of this study.

Although emergency management in other countries is not always organised in the same way as in Sweden, many of the conclusions are general enough to be of importance in an international setting. The increased dependence on IT systems, together with a trend to centralise IT services are commonly found in many countries. The conclusion from this study are therefore likely to be of interest to similar organisations elsewhere that next to their everyday responsibilities also have an active role in crisis relief.

7 PROPOSED PROCESS IMPROVEMENT MODEL

This study shows the need for a method that can help governmental actors improve in how they manage the dependability of their IT systems. More precisely there is need for a process improvement model that is simple enough to be applied by small municipalities, and that is focussed on stimulating the cooperation between the IT personnel and the emergency managers.

One of the possible solutions is the development of a maturity model. A maturity model is a framework for process improvement that includes a number of maturity levels that can be used to evaluate and improve the capabilities of an organisation. Typically, an organisation first evaluates itself on a number of key process areas, and is then assigned a maturity level based upon this evaluation. In the next step, a number of practices necessary for reaching a higher level of maturity can be selected and goals for the next step in process improvement can be set up. This process can be repeated until a desired level of maturity is reached. The top level of maturity is usually a level where mechanisms for continuous improvement are in place.

Based on the experiences from this paper, it can be noted that a maturity model to help organisations measure their current maturity in dealing with these dependability challenges, needs to fulfil a number of special requirements for it to be useful to governmental actors with limited experience in this field. First, it should be possible to use with limited resources, also for small organisations. Secondly, it needs to contain a well-defined self-assessment tool to help organisations to identify and evaluate the processes they use to monitor the dependability of their IT systems. Further, the framework should offer specific, practical examples of good practices that can be used for improvement. Preferably it should be supported by tools for data collection and analysis. Finally, it is also important that the maturity model includes ideas from maturity models already currently in use in both IT management (Luftman, 2003) and in safety culture (Fleming, 2001).

8 CONCLUSIONS AND FUTURE WORK

Through case studies and a survey this paper explores the main challenges involved in how governmental actors, and Swedish municipalities in particular, evaluate the dependability of their IT systems in possible crisis situations. The main contribution of this paper is, first of all, that it identifies the main problems areas in the current state of practice and, secondly, that it sketches the requirements for a process improvement framework that can help organisations improve in these areas.

This study shows that the core of the problem does not lie with either the IT systems themselves or the emergency management procedures, but the real problem is the lack of good cooperation to discuss these matters on a strategical level with all involved parties. Therefore, those responsibilities that lie on the border between different people's areas of responsibility are often given too little attention. This leads to emergency planning that does not incorporate possible dependability problems with IT systems and IT management that does not take into account the special conditions that can occur during emergency situations. These kind of problems cannot be solved by simple measures and require a process improvement effort that involves a large part of the organisation. Because no current framework addresses these issues specifically, we propose the development of a maturity model similar to the process improvement frameworks already in use in some related fields.

REFERENCES

1. Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr C. (2004) Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing*, 1, 1, 11-33.
2. Fleming, M. (2001) Safety culture maturity model. *Offshore Technology Report*, 2000/049.
3. Hallin, P.-O., Nilsson, J. and Olofsson N. (2004) Kommunal sårbarhetsanalys, *KBM:s forskningsserie, 3.*
4. International Organization for Standardization (2005) ISO-IEC 17799: Information technology - Security techniques - Code of practice for information security management.
5. Kalmelid, K., and Gustavsson J. (2005) Inventering av kompetensbehov m.m. inom informationssäkerhet i offentlig sektor, *Technical report, Rapport, Informationssäkerhets- och analysenheten*, Krisberedskapsmyndigheten.
6. KBM (2005) Samhällets krisberedskap - Inriktning för verksamheten 2007, Krisberedskapsmyndigheten, *Planeringsprocessen 2005:3*.
7. Luftman, J. N. (2003) Managing the Information Technology Resource: Leadership in the Information Age, Prentice-Hall.
8. Robson, C. (2002) Real World Research: A Resource for Social Scientists and Practitioner-researchers, Blackwell Publishers, second edition.
9. SEMA (2003) Basic Level for IT Security (BITS), Swedish Emergency Management Agency, *SEMA recommends 2003:2*.
10. Yin, R. K. (2003) Case Study Research: Design and Methods, SAGE Publications Ltd.