

CHALLENGES TO INTRA-ORGANIZATIONAL RISK AND VULNERABILITY INFORMATION FLOW IN PUBLIC ORGANIZATIONS

Borell, Jonas^{1,3} & Eriksson, Kerstin^{2,3}

Lund University, Lund, Sweden

Keywords

risk analysis, vulnerability analysis, intra-organizational communication, information flow, organizational learning

Abstract

As part of risk management efforts aiming at improving safety organizations need to identify risks and vulnerabilities. In Sweden public organizations such as municipalities and county councils shall repeatedly perform risk and vulnerability analyses regarding their own operations as well as their areas of societal responsibilities. Often being large organizations, usually consisting of many hierarchically organized levels and performing diverse activities, these public organizations need to establish aggregated pictures of relevant risks and vulnerabilities that concern the entire organizations. In this study we have examined how four public organizations in Sweden arrange their intra-organizational communication concerning their risk and vulnerability analyses. The aim was to study challenges that the organizations perceived concerning intra-organizational information flow in relation to their risk management efforts. The study is based on interviews with key personnel responsible for design and management of work procedures for risk and vulnerability analyses. Data are analyzed and interpreted using theories of communication and management. All four organizations reported experiencing risks concerning misinterpretations of reported messages within their work processes. There were also some apprehensions that ultimate aims with the work might not be reached, due to sub-optimal set-up of work processes. Implications of the findings are discussed and general suggestions for the design and managing of information flow in large, hierarchically organized systems for risk and vulnerability analysis are pointed out.

Introduction

Modern societies take many measures to protect themselves and their citizens from emergencies. When the society strengthens its abilities to manage emergencies and to continue critical operations, analyses of risks and vulnerabilities play a central role (ISO, 2007). In recent years Sweden has formed a national system, aiming at increasing societal safety and security. Legislation (SFS 2006:544) states that all Swedish authorities shall repeatedly perform risk and vulnerability analyses. All authorities also have to define their

¹Department of Design Sciences, Division of Ergonomics and Aerosol Technology, Lund University, P.O. Box 118, SE-221 00 Lund, Sweden, jonas.borell@design.lth.se

² Department of Fire Safety Engineering and Systems Safety, Lund University, P.O. Box 118, SE-221 00 Lund, Sweden, kerstin.eriksson@brand.lth.se

³ LUCRAM (Lund University Centre for Risk Assessment and Management), <http://www.lucram.lu.se>

critical functions (SFS 2006:942), with special focus on the identification of functions that are necessary for preventing, or when responding to, serious emergencies. A fundamental principle in the Swedish system is that the authority with responsibility for a particular activity is responsible for ensuring a basic level of functionality, meaning that the activity is capable of withstanding and managing disruptions and emergencies. The new Swedish legislation applies to all levels of society, from local authorities (municipalities), over regional (county councils and county administrative boards), to central authorities (e.g. governmental agencies); All authorities have to perform risk and vulnerability analyses and to assess their emergency management capabilities. In the national system for increasing societal robustness and safety, each authority (e.g. county council or municipality) shall annually report to the national government which actions they have taken to decrease risks and vulnerabilities.

Given these external demands, we have investigated how four public organizations interpret what they are supposed to do concerning their mandatory risk and vulnerability analyses. Two of the organizations are county councils, and two are municipalities (Some characteristics of the four organizations are presented in table 1). We wanted to know how these public organizations view their own duties and activities. In particular, we wanted to know what challenges and potential problems they experience. The aim of this paper is to describe challenges that the organizations perceived concerning intra-organizational information flow in relation to their risk management efforts, and to discuss this in light of theories of organizational communication and learning. In the long run, this research aims to contribute to the improvement of societal emergency management processes.

Table 1. The organizations studied

	<i>Organization</i>			
	A	B	C	D
<i>Kind of organization</i>	County council	County council	Municipality	Municipality
<i>Approx. no. of citizens served</i>	1,5 million	1,2 million	300 000	100 000
<i>Approx. no. of employees</i>	50 000	33 000	19 000	9 000
<i>Organization's own interpretation of aim with risk and vulnerability work</i>	Robust operations. Ability to manage risks; Administrations should learn and develop.	Improve operational continuity and formal reporting of risk and vulnerability status to central authorities.	Good emergency preparedness and capability to manage events that "lay outside everyday operations".	Improve municipal emergency management capability and robustness.
<i>Roles of central staff and administrations</i>	All administrations shall report A) a self-assessment of emergency management capability to central unit and B) "any common risks, that need to be managed across administrations' borders".	All administrations shall report results from risk and vulnerability analyses to central unit.	All administrations shall report results from risk and vulnerability analyses to central unit.	All administrations shall perform risk and vulnerability analyses in cooperation with central unit.

Theory

Swedish municipalities arrange, among other things, social welfare, care for elderly, schooling, and provide fire and rescue services. They also have a general responsibility for the wellbeing of all inhabitants and visitors. Swedish county councils arrange health care, public transportation, cultural activities and regional economical development programs. Swedish county councils and municipalities are usually organized with central management, and operations run in different administrations. The administrations are usually built up by different businesses, which run actual operations. The result is an organizational structure in the form of a 'classical' hierarchical pyramid. This structure characterizes all four organizations included in this study.

Being large and hierarchically organized systems, obliged to analyze themselves and report to central authorities, the studied organizations need some kind of reporting structure that can be viewed as a hierarchical system for risk and vulnerability analyses. With the legislated demands being a few years old, most Swedish authorities are still designing and trimming in their first generations of solutions to the new demands. The organizations studied here are quite typical in having performed their first real iteration of analyses in 2008.

In table 1 the studied organizations' interpretations of aims with their mandatory risk and vulnerability work are given. In order to fulfill these aims it is necessary to perform "second order analyses" (Eriksson & Borell, 2008) at the top of the hierarchies, i.e. there is a need to compare and merge analysis-results from lower levels. This means that it is not sufficient to simply add or aggregate information, but necessary with new analyses, employing level-specific questions and methods.

When performing second order risk and vulnerability analyses at the top level of hierarchical organizations as the ones studied here, situational sensemaking is critical. Sensemaking is the function of gathering relevant information, performing adequate considerations, and deciding on action (Weick, 1995). On the level of individuals sensemaking is dependent on expectations, which provide a frame of reference (Ibid). Which goals and aims one is aware of guides ones understanding and acting. Accordingly, proper construction, gathering, processing and utilization of risk and vulnerability information requires a well established sense of the ultimate purpose to which the task at hand is instrumental. Therefore it is crucial in designing work processes for hierarchical systems for organizational risk and vulnerability analyses to provide appropriate conditions for successful sensemaking.

What an individual is capable of in a certain situation is dependent on which aspects of the situation the individual is focally aware of. This, in turn, is dependent on the set of dimensions, among all the inexhaustible possibilities, that the individual is able to simultaneously discern and become aware of. An individual's ability to experience a situation in a particular way, i.e. to become simultaneously aware of certain aspects in the situation, comes from that individual's earlier experiences. Having perceived variation regarding a dimension of possible variation enables a person to later discern that particular aspect in future situations. (Marton & Booth, 1997) An individual who is to perform second order risk and vulnerability analyses (Eriksson & Borell, 2008) ought to be equipped with experiences enabling a proper sensemaking for the task, e.g. able to assign a suitable frame of reference for interpreting information.

Work processes are systems of linked actions arranged together for a certain purpose. Design of work processes can be done using design logic (see figure 1), wherein one starts with the overarching *purpose*; what is the *raison d'être* of the work process? Thereafter a set of *functions*, together forming a coherent whole believed to deliver the sought result, is identified and described. The final step is to assign *form* through choosing what activities, corresponding to the functions identified, that should be implemented for actual operations. Such a system comprising purpose, functions and activities can be represented as an

“abstraction hierarchy” (Rasmussen & Lind, 1981), helping in managing complexity through the use of aggregation of information.

Figure 1. The principles of design logic, represented as an abstraction hierarchy



The design and management of work processes is crucial to organizational performance, which can be measured through how well the output of an organization’s processes matches its desired outcome (Rummler & Brache, 1995). Bad design or management of work processes make satisfactory fulfillment of an organization’s purpose less probable.

Actual organizations often comprise several work processes, linked together in a system. Overall system performance is then dependent on system integration, which means that processes are interconnected and output from one process is fed in as input to another process. Ultimate success demands that “loops are closed” (e.g. Kjellén, 2000) and, for example, that output from a risk and vulnerability analysis process is utilized in decision making and eventual implementation.

If organizational work around risk and vulnerability analyses is supposed to render knowledge, and the work comprises a sequence of several distinct steps, the entire work process ought to be optimized for knowledge creation. In processes comprising several consecutive steps, knowledge cannot be transmitted as such, but has to be codified as information and transmitted as a message from a sender to a receiver (Davenport & Prusak, 2000). Success is reached if the receiver manages to interpret a message in such a way that acceptably similar knowledge is reached as held by the sender.

A large part of the valuable knowledge borne by organizational members is in the form of tacit knowledge, which is not possible to put in formal, written reports. Therefore it is of special interest to arrange opportunities for tacit knowledge to be transmitted between individuals, and to be transformed into explicit knowledge (Nonaka & Takeuchi, 1995). In the case of work processes for organizational risk and vulnerability analyses it is worth striving for utilization of tacit knowledge.

Coordinated behavior and effective communication in organizations require that different organizational members understand each other. A prerequisite for mutual understanding is shared meaning structures, which are developed by interactions wherein individual’s private meaning structures are exposed and responded to by other organizational members (Dixon, 1999). Hierarchical reporting systems for risk and vulnerability analyses should contain, or be complemented by, functions that promote the construction of shared knowledge structures.

When organizations are strictly arranged around divisions it is not unusual that “silo effects” occur. Silo effects are when different parts of an organisation have very vague understandings of each others functions and conditions, which hinders effective communication and cooperation across division borders (Dixon, 1999). Silo effects may be countered by a management philosophy that focuses on work processes (Rummler & Brache, 1995), and thus emphasizes how operations can be optimized involving all organizational divisions. Providing functions that let individuals share opinions and understandings collectively may build collectively shared understandings in the form of shared meaning structures (Dixon, 1999), which also function as a basis for cross-divisional cooperation.

Method

The aim of this paper is to describe challenges that four Swedish public organisations perceived concerning intra-organizational information flow in relation to their risk management efforts, and to discuss this in light of theories of organizational communication and learning.

Data was collected through interviews with persons⁴ responsible for the development and management of work processes for risk and vulnerability analyses. The interviews were semi-structured and performed with both authors present. The interviews were recorded.

Data analysis was performed through both authors listening to the interview recordings independently, using a common analysis guide. Findings were compared with theories on communication and organizational as well as individual learning.

With all four organizations the authors have performed other studies before, around associated themes. This has provided the researchers with extensive background knowledge about the organizations and their different efforts concerning safety and security issues.

To enable analysis and comparisons between the organizations studied we have chosen to discuss in terms of work processes. None of the four organizations explicitly communicated in terms of work processes. Therefore our use of representations in process form rests on interpretations of the information provided in the interviews together with background knowledge about the organizations.

The aspects of communication/information flow and organizational learning were considered central to successful implementation of organizational systems for risk and vulnerability analyses, and therefore used to further structure description and analysis.

Results

A summary of challenges to information flow and proper functioning of the risk and vulnerability reporting systems expressed by the informants is given in table 2 below.

Table 2. Challenges to information flow and proper functioning of the risk and vulnerability reporting systems expressed by informants

	Potential problem, as expressed⁵ by (Organization)	Solution expressed by the organization
1⁶	Fear of miscommunication due to misinterpretation of reported information. (C)	Let some persons participate in several consecutive steps of the overall work process, in attempt to minimize misinterpretation of reported information.
2	“Communication problems”, where messages are not interpreted by receiver as intended by sender; Interpretation and valuation of information at intermediate levels in the hierarchical reporting system might render [unintentional] distortions of original message. (B)	No <i>direct</i> solution expressed.
3	Deliberate misuse of system, in order to either hide shortcomings for top management and public, or to gain extra funding for exaggerated problems. (A)	Considered a “non-problem”; If excessively <i>positive</i> image is given, efforts to change actual status to be in accordance with what is reported is expected. Excessively <i>negative</i> image is not considered probable. Furthermore, the central organization also uses informal contacts and other data sources to check reliability of formally

⁴ Two persons from each of organizations A and D, and one from each of organizations B and C.

⁵ Formulations in table are condensed and sometimes reworded compared to actual statements in interviews.

⁶ Numbers only intended for reference.

Potential problem, as expressed ⁵ by (Organization)	Solution expressed by the organization
4	reported information. No <i>direct</i> solution expressed.
5	Avoid revealing specific administrations' shortcomings in municipal-level report. Keep the reported material from administrations as "working material", i.e. not public.
6	Awareness of the potential problem, and preparedness to by-pass the annual reporting system if findings call for urgent measures. Arranges cooperation between organizational entities beside the formal reporting loop, in attempt to facilitate swift measures.
7	Attempts to [remind oneself to] return to main aim as guide for analysis/Aligning sensemaking with top mission.
8	No <i>direct</i> solution expressed. for how to ensure that "loops are closed" and analysis results properly utilized.
9	Arranges forum for cooperation between different administrations. [Counter-measures aimed at "silo-effects".]

Discussion

The different problems can be logically grouped according to theme. Problems 1-5 all concern different aspects of communication taking place within the work processes. Problems 6-9 concern possible failures to effectively achieve the final aims of the work performed.

All four organizations aim at increasing robustness and/or their emergency management capability. The studied organizations all use rather rationalistic approaches. They collect data, gather information in reports, send documents between different levels/units in the organizations etc. In one way or another, all four organizations placed information flow in focus when describing their work, work processes and perceived challenges to successful implementation. However, none of the interviewed persons expressed the intended outcomes of the work processes in terms of collective learning or the establishing of future capacity for certain awareness.

For problem 1 organization C reported a solution where communication is strengthened by letting some individuals take part in several consecutive steps of the work process, and thus carry a fairly large amount of associated tacit knowledge that facilitates an accurate interpretation of explicitly reported information. Organization C lets process leaders for risk and vulnerability analyses, who are affiliated to the central organization, be involved in performing analyses within the administrations, and later also participate in central "analysis of analyses" activities. (Organization D uses a similar solution, but did not report any problem as reason for it.) This does not only allow the process leaders to carry information. It also provides interaction with representatives from the reporting/sending part (the administration), which enables tacit knowledge to be transmitted that is not codified in the official reports.

This is an example of good organizational communication, possible to render knowledge creation and thus organizational learning (Nonaka & Takeuchi, 1995).

The reported problems concerning the potential for deliberate misuse of the system may be partly mitigated by tackling 'silo effects'. It is possible that an enhanced understanding between parts of an organization decreases the probability for unintended as well as deliberate communication problems.

Problem 7, reported by organization B, can be analyzed as concerning sensemaking in the function of analysis of analyses. The problem was expressed as a possibility to loose focus and get distracted by content in the analysis reports received from lower hierarchical levels. The solution proposed was to keep an awareness of the potential problem, and remind oneself of the main purpose every now and then.

It seems possible that the organizations studied may suffer from not truly integrated management systems, with unclosed loops. Some of them expressed awareness of the possibility. For example, organization D reported a fear that some suggested improvements might not happen, due to distribution of decision power not aligned with the responsibility for the risk and vulnerability analysis process (problem 8 in table 2). The informants from organization D also mentioned that they wish that findings from the municipality's hierarchically arranged risk and vulnerability analyses should find its way down again, and affect the bottom line of the organizational pyramid. They did not, however, have any plans or general ideas for how to arrange that. This constitutes an obvious lack in organization D:s work process, since they want it to deliver increased municipal emergency management capability.

In the interviews much was reported on the level of form, concerning tangible work tasks within the different organizational systems for risk and vulnerability analysis. There was also some focus on the level of functions identified as relevant for proper functioning. However, there were rather few references to the purpose of the systems. It is probable that a more systematic approach to the designing of their work processes, perhaps using 'design logic', would yield more valuable output.

What has been reported in the interviews can by no means be treated as exhaustive accounts of all challenges and potential problems the studied organizations face or even are aware of. It is probable though that the spontaneous replies given in the interviews correspond to conceptions given high priority. Therefore the gathered pool of expressed threats is probable to reflect a set considered important. It may very well be the case that all problems reported in reality apply to all four organizations studied, even if this was not reflected in the interviews.

This study is of Swedish organizations working under Swedish legislation. We have not seen any obvious reasons for the findings to not be applicable to other cases sharing the same characteristics, e.g. hierarchically organized systems for risk and vulnerability analysis reporting in large organizations.

From theory some general conclusions can be drawn. For example, it is necessary to process information properly. However, this is not sufficient. For ultimate success it is also necessary to aim at creating knowledge, possibly in the form of potential for appropriate awareness. This means that work processes ought to be optimized for these criteria. Furthermore, interaction is necessary for efficient and reliable communication. It is not recommendable to see and treat work process as built up by distinct steps without overlap. Finally, it doesn't help that information is transferred and proper analyses are performed, if loops are not closed and work processes are not interconnected properly. In the organizations studied, problems as well as solutions related to all of these areas were found. Further studies, using more cases and more extensive analyses would render valuable insights into how to improve societal efforts at increasing safety.

References

- Davenport, T. H. & Prusak, L. (2000). *Working knowledge: how organisations manage what they know*. Boston, Harvard Business School Press.
- Dixon, N. M. (1999). *The organizational learning cycle – How we can learn collectively*. Aldershot, Gower.
- Eriksson, K. & Borell, J. (2008). Second order risk and vulnerability analyses. *Proceedings of TIEMS 15th annual conference*, TIEMS.
- ISO. (2007). *Societal security - Guideline for incident preparedness and operational continuity management*. ISO 22399:2007(E).
- Kjellén, U. (2000). *Prevention of accidents through experience feedback*. London, Taylor & Francis.
- Marton, F. & Booth, S. (1997). *Learning and awareness*. Mahwah, NJ: Lawrence Erlbaum Associates.
- Nonaka & Takeuchi. (1995). *The knowledge-creating company*. Oxford: Oxford University Press.
- Rasmussen, J., & Lind, M. (1981). *Coping With Complexity*. Risø-M-2293. Risø National Laboratory, Denmark.
- Rummler, G. A. & Brache, A. P. (1995). *Improving performance: How to manage the white space on the organization chart*. (2nd edition) San Francisco, Jossey-Bass.
- SFS 2006:544, *Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*, Svensk Författningssamling. (In Swedish.)
- SFS 2006:942, *Förordning om krisberedskap och höjd beredskap*, Svensk Författningssamling. (In Swedish.)
- Weick, K. E. (1995). *Sensemaking in organizations*. Thousand Oaks, California, Sage Publications.

Author Biographies

Jonas Borell is a PhD student at the Department of Design Sciences at Lund University. Jonas has a MSc in Psychology. His main research area is proactive safety management.

Kerstin Eriksson obtained her Licentiate degree in Engineering in 2008 and her MSc in Risk Management and Safety Engineering in 2004. She is currently a PhD student at the Division of Fire Safety Engineering and Systems Safety at Lund University, Sweden. Her research is focused on emergency preparedness and management.

Both authors are active in FRIVA, a framework research program funded by the Swedish Emergency Management Agency.