IS Capability for Incident Management and the DERMIS Design Premises

Gerd Van Den Eede
Vlekho Business School, Brussels, Belgium
gvdeede@vlekho.wenk.be

Willem Muhren, Raphaël Smals and Bartel Van de Walle
Tilburg University, The Netherlands
{w.j.muhren, r.g.m.smals, bartel}@uvt.nl

ABSTRACT

In this paper we present a dynamic model of the performance of an organization's Incident Management process as determined by the capability of its supporting emergency response information system. Our work is based on the Capability Trap model by Repenning & Sterman (2001) and draws from the many insights on emergency response information systems design as described in the DERMIS (Dynamic Emergency Response Management Information System) framework established by Turoff *et al*. 2004. Whereas the latter describes the premises that underlie an Information System (IS) that is capable of ensuring a reliable and flexible emergency response, the present paper contributes to the research field by looking at the interrelations of the aforementioned premises. We take a System Dynamics approach and gain insights in the key determinants of IS Capability by highlighting the mutual interdependences grouped around the concepts of adaptability, control, implicit knowledge and explicit knowledge.

Keywords

Incident Management, Dynamic Emergency Response Information Systems, Capability trap, System Dynamics, ISCRAM.

INTRODUCTION

In this paper, our objective is to analyze the performance of an organization's Incident Management process as influenced by the capability of its emergency response management information system, which is in turn determined by the design characteristics the organization uses to handle (route, document, communicate, …) its incidents. In order to do so, we make use of System Dynamics (SD) modeling. SD allows us to facilitate insight and communication about organizational issues (like performance, targets, interactions, link between strategic and operational level) without completely eliminating complexity as in a business game (Canon et al. 1995). System Dynamics fosters complexity and offers an antidote for linear thinking, as for instance in the assumption "*if we increase salary of incident workers, the quality of the Incident Management process will improve*".

The starting point for our IS Capability modeling purposes was found in the work of Repenning and Sterman (2001) which offers ways of breaking out of the so-called Capability Trap in order to achieve process improvement. Our attention towards the underlying dilemma of 'working hard' versus 'working smart' was first drawn from work of Sawicka et al. (2005) in their application of the original insights into the field of capability of Computer Security Information Response Teams (CSIRT). Whereas Sawicka et al. focus on the management of CSIRT capacity as a renewable resource, we wish to study how the Incident Management process is impacted by the design of incident response information systems.

The basic idea behind the 'working hard' versus 'working smart' dilemma is that management tends to choose for a 'working hard' strategy because this yields a direct result on performance whereas a choice for a more proactive

investment in capability enhancement will only bear fruits after a much longer period of time. As Figure 1 shows, in the long run performance of the working smarter strategy will outpace its working harder equivalent.

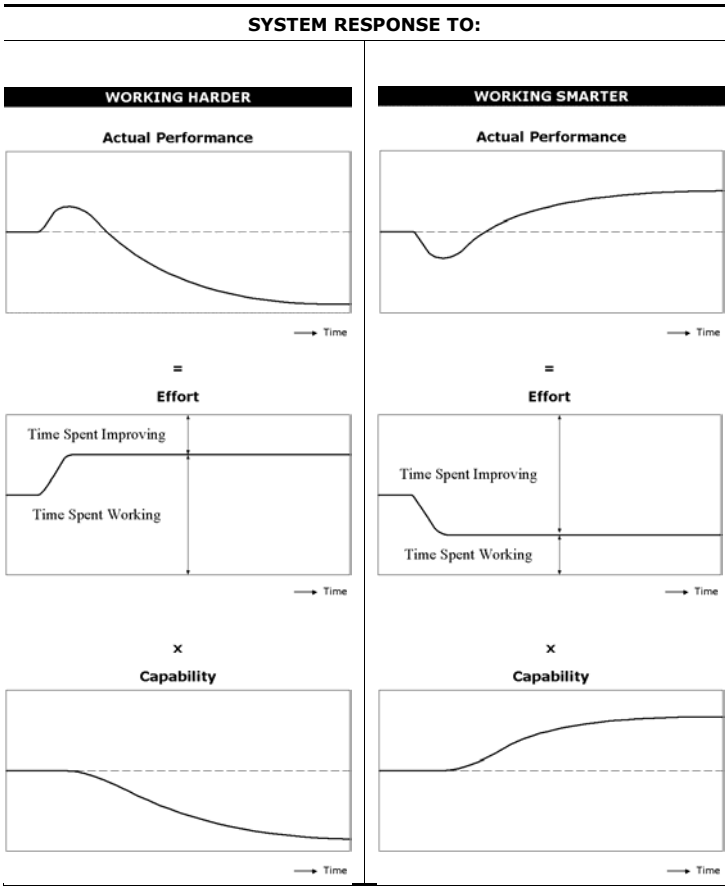

Figure 1 The Capability Trap (Adapted from Repenning & Sterman 2001)

INFORMATION SYSTEMS CAPABILITY

The goal of Incident Management is to restore normal service to operation as quickly as possible with minimum disruption to the organizational processes, thus ensuring that the best achievable levels of availability and service are maintained (CCTA 2000, p. 71). Incident Management should be used to ensure the best use of resources to support the organization, to develop and maintain meaningful records relating to incidents, and to devise and apply a consistent approach to all incidents reported. Incident Management is responsible for incident detection and recording, classification of all incidents, and initial support, investigation and diagnosis, resolution and recovery, incident closure, and incident ownership, monitoring, tracking and communication (CCTA, p. 71). Incidents range from minor disruptions to full-scale emergencies/crises.

Even though information technology has evolved from being a mysterious part of the business that resided deep within the bowels of an organization to being the backbone of virtually every industry (MacInnis 2005), to date, IS literature has not defined IS capability beyond "an expression of its core objective of enabling an organization to continuously derive and leverage business value through IS/IT" (Peppard et al. 2004). Nor has it described the fundamental components or characteristics of organizational IS capability.

In this paper we attempt to describe the IS capability characteristics from the perspective of its users. In particular, a user has to:

1. *Learn from the IS*
2. *Adapt the IS*
3. *Document the process through the IS*
4. *Control the IS*.

The IS Capability Model in Figure 2 shows these characteristics as interrelated determinants of IS capability. In order to gain insight in the way these variables influence each other, we have built a System Dynamics (SD) model that incorporates the possible relationships between these variables. We do not argue that the above characteristics are exhaustive, nor that they are exclusive. However, we take them as a starting point for examining the properties of IS capability and the way this influences organizational performance.

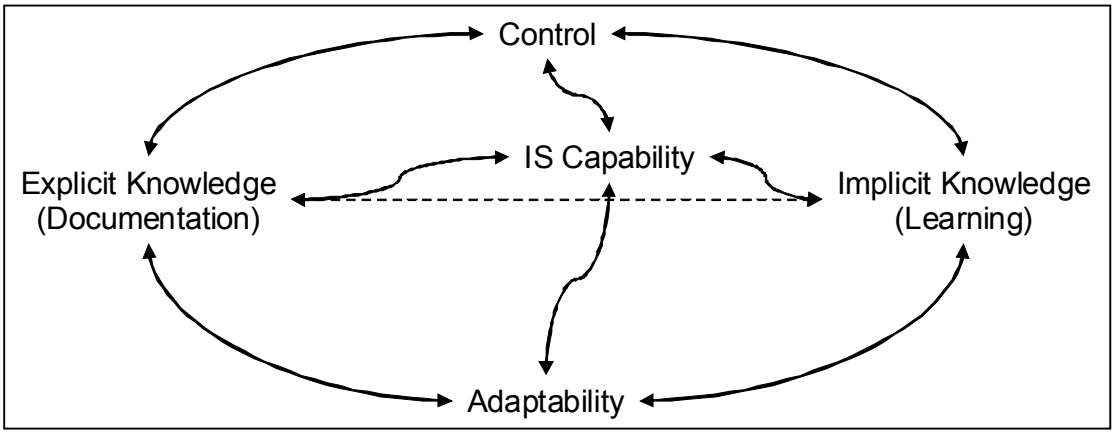

Figure 2 Proposed IS Capability model

DERMIS DESIGN PREMISES

Management processes are acts of coping with a wide variety of complicated or even complex issues. In this respect, management is convinced of being *on top of things* and steers the organization from a control cockpit – as is reflected in the widespread use of tools and philosophies like the Balanced Scorecard. This worldview is translated in the way the processes and the underlying information systems (IS) are designed. Yet, deployment of processes and IS does not always seem to show a satisfactory result in terms of performance (i.e. flexibility or even reliability). However, this does not seem to disturb designers and managers as there is no noticeable change in their conduct. "*The comforting illusion of control over an uncontrollable world is a powerful one*" (Powell, unpublished, quoted by McLucas 2003, p. 21). This is reinforced by the fact that when things are going well, management does not experience a stimulus to change its worldview and that when things are not going well, the pressure to continue working harder instead of smarter is increasing (Repenning and Sterman 2001). The dominant worldview thus is reinforcing itself. A *tour-de-force* of complex intervention seems to be necessary to change this reinforcing tendency. We here use the DERMIS design premises for emergency response information systems as developed by Turoff *et al*. (2004), and a brief overview of which is given in Table 1.

Table 1 DERMIS Design Premises (Turoff *et al.* 2004)

P1 SYSTEM TRAINING AND SIMULATION. Turoff et al. argue that finding functions in the emergency response system that can be used on a daily basis, is actually much more effective than isolated training sessions. Indeed, if the system is used on a day-to-day basis, this will partly eliminate the need for training and simulation, as those who must operate the system, gain extensive experience with the system just by using it.
P2 INFORMATION FOCUS. During a crisis, those who are dealing with the emergency risk are flooded by information. Therefore, the support system should carefully filter information that is directed towards actors. However, they must still be able to access all (contextual) information related to the crisis as information elements that are filtered out by the system may still be of vital importance.
P3 CRISIS MEMORY. Furthermore, it is important that the system is able to log the chain of events during a crisis, without imposing an extra workload on those involved in the crisis response. This information can be used to improve the system for use in future crises, but it can also be used to analyze the crisis itself.
P4 EXCEPTIONS AS NORMS. Due to the uniqueness of most crises, usually a planned response to the crisis cannot be followed in detail. Most actions are exceptions to the earlier defined norms. This implies that the support system must be flexible enough to allow reconfiguring and reallocation of resources during a crisis response.
P5 SCOPE AND NATURE OF CRISIS. Depending on the scope and nature of the crisis, several response teams may have to be assembled with members providing the necessary knowledge and experience for the teams' tasks. Special care should also be given to the fact that teams may only operate for a limited amount of time and then transfer their tasks to other teams or actors. The same goes for individual team members who may, for example, become exhausted after an amount of time.
P6 ROLE TRANSFERABILITY. As said above, individuals should be able to transfer their role to others when they cannot continue to deal with the emergency. For the support system, this means that clear descriptions on roles must be present, as well as a description of the tasks, responsibilities and information needs of each role.
P7 INFORMATION VALIDITY AND TIMELINESS. As actions undertaken during crises are always based on incomplete information, it is of paramount importance that the emergency response system makes an effort to store all available information in a centralized database. Thus, those involved in the crisis response can rely on a broad base of information, helping them making decision that are more effective and efficient in handling the crisis.
P8 FREE EXCHANGE OF INFORMATION. During crisis response, it is important that a great amount of information can be exchanged between stakeholders, that they can delegate authority and conduct oversight. This, however, induces a risk of information overload, which in turn can be a risk to the crisis response effort. The response system should somehow protect participants from information overload.
P9 COORDINATION. Due to the unpredictable nature of a crisis, the exact actions and responsibilities of individuals and teams cannot be determined ex ante. Therefore, the system should be able to support the flow of authority directed towards where the action takes place (usually on a low hierarchical level), but also the reverse flow of accountability and status information upward and sideways through the organization.

Linking IS Capability and DERMIS

The design premises from Table 1 describe the characteristics of an IS that is capable of ensuring a reliable and flexible emergency response. This description however limits itself to the level of the individual components. It does not make an attempt of describing the interrelations that (might) exist between them. The present paper takes up this challenge and as such makes an attempt to contribute to the ISCRAM research field. We take a System Dynamics approach to gain insights in the key determinants of IS Capability. For that matter we highlight the mutual interdependences grouped around the concepts of adaptability, control, implicit knowledge and explicit knowledge.

1. ***Learn from the IS*** so that at no occasion it will be novel, hence dissolving the unnatural discrepancy between day-to-day loosely-coupled and task-oriented behavior on the one hand and supposedly rule oriented logics of action (Snook 2002) when the situation becomes tightly coupled in case of an exceptional event on the other hand. This idea is expressed under P1 and relates to the notion of ***Implicit Knowledge***

2. ***Adapt the IS*** in order to make it suitable for accomplishing the 'task' without disobeying the 'rule'. This idea is expressed under P2, P4, P5 and P6 and relates to the notion of ***IS Adaptability***
3. ***Document the IS*** in such a way that it provides sufficient and easily constructible information in order to avoid parallel handling of events outside the system when the situational coupling (Snook 2002) gets tight. It is not in loosely coupled situations that the need for an adequate documentation is felt the most (because in such cases there will always be sufficient slack in the system to cope with insufficient documentation), but it is when the situation gets tightly coupled (resulting in little time, little degrees of freedom to organize work, …) that the system should provide the information required to handle the abnormality. This idea is expressed under P3 and P7 and relates to the notion of ***Explicit Knowledge***
4. ***Control the IS*** in such a way that inevitable deviations from foreseen procedures is allowed for/facilitated by the system and that it provides sufficient ways of communication. This provides an antidote for scope narrowing and threat rigidity and will succeed in aligning a task-oriented approach with a design perspective. This idea is expressed under P8 and P9 and relates to the notion of ***Control***.

IS CAPABILITY FOR INCIDENT MANAGEMENT PERFORMANCE

We develop a System Dynamics model in which we integrate the nine DERMIS design premises to analyze the performance of the Incident Management process by focusing on the interdependences between them . An overview of the complete model is given in Figure 3, yet for the reader's convenience the model will be 'decomposed' in sectors and discussed in more detail in the following subsections.

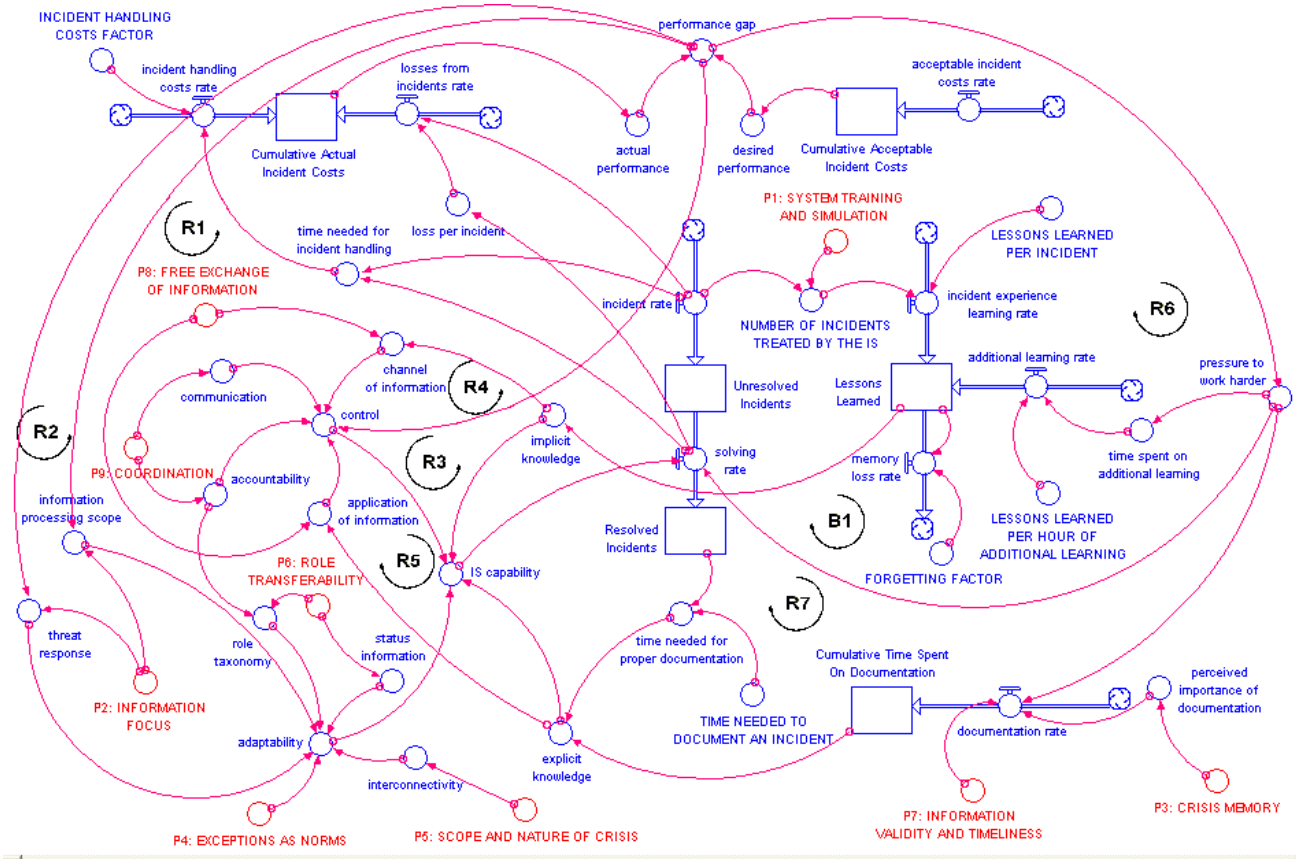

Figure 3 Full IS Capability Model

Performance

The core of the generic SD model is the performance of the Incident Management process as shown in Figure 4.

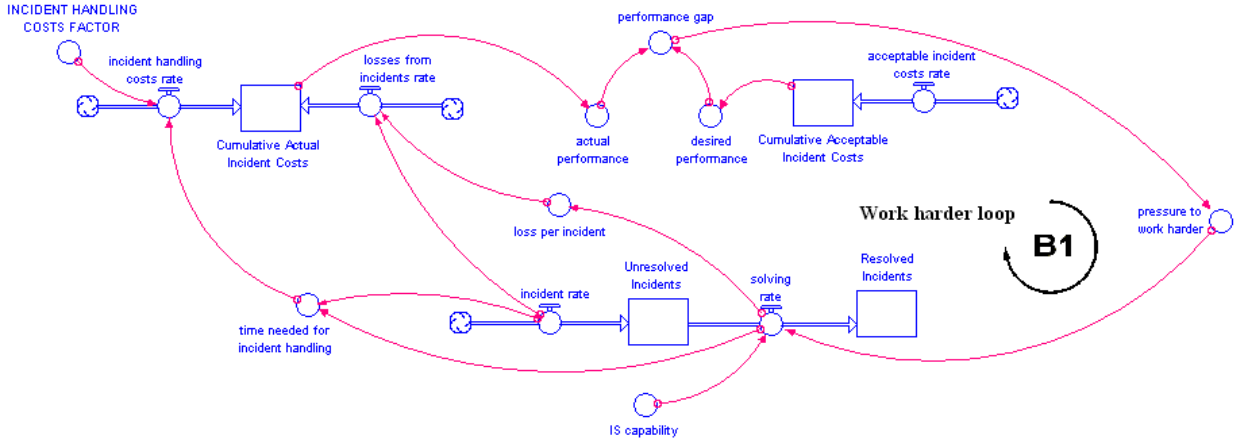

Figure 4 Performance sector: Incident Management Process Performance and IS Capability

Consistent with the definition of IS Capability by Ward and Pepper (2002), we define IS Capability in our model as the degree to which the IS is successful in delivering business value, i.e., an increase in solving speed is obtained as a result of IT/IS investments. The solving rate of incidents – the speed at which incidents are correctly solved – affects the losses from incidents rate (the quicker an incident is solved, the less damage it causes) and the time needed for incident handling. The actual performance of the Incident Management process is the inverse of the financial consequences of the Incident Management process: the sum of labor costs of managing the process (incident handling costs rate) and the damage the incidents cause (losses from incidents rate). The desired performance reflects the acceptable incident costs, the management's financial target of the process. The performance gap is the difference between the actual performance and the desired performance. Management will constantly try to close the performance gap by pressuring people to work harder (Repenning & Sterman 2001). This will result in an increase in speed of the incident response and over time a decrease in costs and thus an increase in performance, shown by the *Balancing Work harder loop* (B1).

In our model IS capability is not an exogenous variable but is determined by four other variables: Adaptability, Control, Implicit Knowledge and Explicit knowledge. Their relationships with IS Capability will be explained in the following subsections.

First determinant of IS Capability: Adaptability

It has been acknowledged that any gain in the programmability of information processing is achieved at the expense of its adaptability and its computational efficiency, and vice versa. This is known as the adaptability-programmability tradeoff principle (Kampfner 1998, p. 154). An advanced IT-supported process thus generally suffers from a reduction of its adaptability to respond to different circumstances, which in its turn has a negative impact on quality. IS Adaptability groups four DERMIS design premises: P2, P4, P5 and P6. They are interrelated through feedback loops, to each other or to other model components as can be seen in Figure 5.

The first component is the Information Focus design premise (P2) which consists of an Information Processing Scope and Threat Response. Information Processing balances on the thin line between not too much information (information overload) and sufficient information. Rudolph and Repenning (2002) have examined the effect of information overload on crisis management (in particular stress) from a System Dynamics perspective. Based on DERMIS, we add to this discussion by pointing out the reinforcing effect of the performance gap not only on the information processing scope (R1 *Information Processing Loop*) but also on threat rigidity (R2 *Threat Response Loop*). A performance gap, for instance, will lead to a narrowing of the information processing scope (Staw *et al.* 1981), which in its turn will lead to a reduction of the IS adaptability because of a more limited usability in less

different circumstances. The danger of a rigid response to threat follows a similar pattern for example when the performance gap becomes larger. This is a plea for working smarter instead of working harder. This could be achieved by creating the enabling conditions for such a response, notably a loosening of control and a widening of the availability of resources and information (See e.g. Sutcliffe and Vogus (2003) for a study of these conditions).

The second component is the Exceptions as Norms design premise (P4). This means that the end user must be able to reconfigure the system interaction in a dynamic manner and designate changes in priorities, filtering and delivery options at any moment during the emergency management process. It also means the system has to dynamically observe these changes and keep others who need to know about them up to date (Turoff *et al*. 2004, p. 8).

The third component is the Scope and Nature of Crisis design premise (P5), meaning that the critical problem of the moment is requiring people, authority, and resources to be brought together at a specific period of time for a specific purpose (Turoff *et al*. 2004, p. 8). This design premise is all about connecting people in an organic (i.e. dynamic, non-static) way.

The fourth component is the Role Transferability design premise (P6) and consists of knowing who can fulfill which role (role taxonomy) but also of knowing who is available at the time of action (status information). Knowing what data relative to a problem is current, what the source is, and what is its degree of accuracy or status of the data is as important as the data itself. Concepts such as roles, responsibilities and the explicit status variables of the data and roles (priority, accuracy, source, actions, interests, concerns, etc.) have to be part of the collaborative database supporting the operation. It is in this respect that role taxonomy interrelates to the Control Determinant. If adaptability is about delegation and changing roles, the accountability issue becomes very dominant since real delegation consists of responsibility and the resulting accountability.

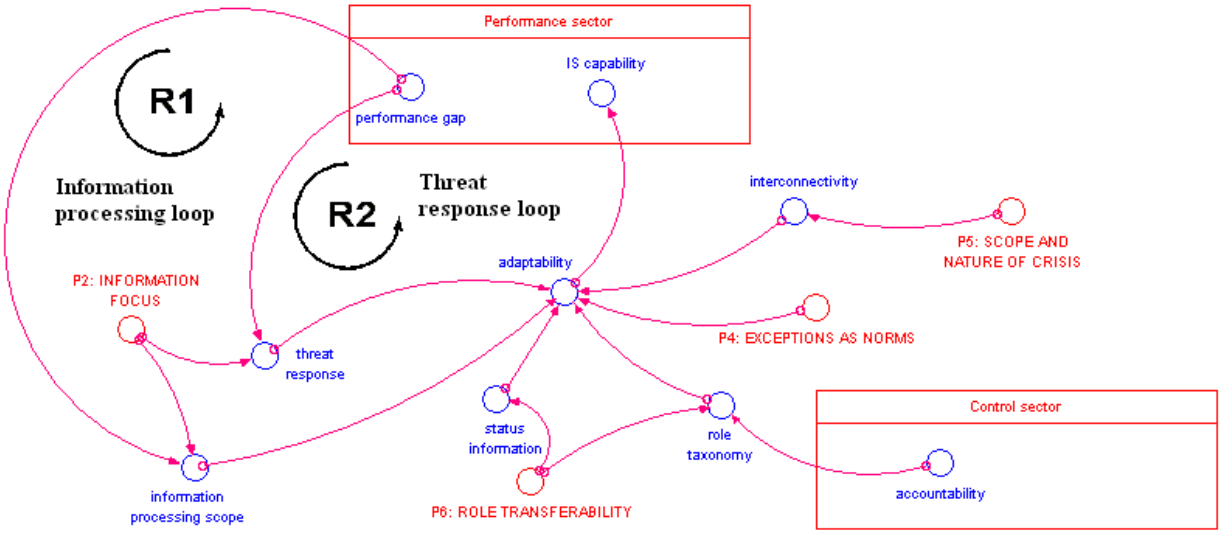

Figure 5 Adaptability sector: Adaptability Determinant of IS Capability

Second determinant of IS Capability: Control

The first component of the Control Determinant is the Free Exchange of Information premise (DERMIS design premise P8). During crisis response, it is important that a great amount of information can be exchanged between stakeholders, that they can delegate authority and conduct oversight. This, however, induces a risk of information overload, which in turn can be a risk to the crisis response effort. The response system should somehow protect participants from information overload. This implies a great deal about the functionality designed in an emergency response system (channel of information). This refers to the quantity and quality (properties) of the available information sources and channels. An equilibrated IS manages to find a balance between sufficient information and not too much information (Staw *et al.* 1981). It infers, for example, that the data and actions in such a system must

clearly be identified by who is supplying an idea, a plan, a viewpoint, data and/or taking an action (Turoff *et al*. 2004, p. 11). We refer to this as application of information.

The second component of Control is the Co-ordination premise (DERMIS design premise P9) which in its turn consists of the accountability and the communication variable. Due to the unpredictable nature of a crisis, the exact actions and responsibilities of individuals and teams cannot be determined ex ante. Therefore, the system should be able to support the flow of authority directed towards where the action takes place (usually on a low hierarchical level), but also the reverse flow of accountability and status information upward and sideways through the organization.

Three reinforcing loops can be noticed:

1. a *Control loop* (R3) that results in an upward or downward impact on IS Capability and performance if the Control parameter is more or less adjusted (i.e. a balance between free exchange of information and co-ordination). This insight builds on the Threat-rigidity thesis (Staw *et al.* 1981) which states that people who are involved in a crisis situation (of some sort) exhibit a rigid response to threat when control is tightened, resources are restricted and dissemination of information is restrained. Reinforcement loop R3 represents Loosening-up of these parameters which acts as an antidote that reinforces IS capability.
2. a *Channel of information loop* (R4) that results in an upward or downward impact on work pressure, which in its turn leads to less or more time to learn. This experience building will increase the flexibility because the threat 'response tool-kit' will be enhanced by new scenarios and heuristics. The existence of such rules and awareness allows for a broad use of the possibilities offered by the available channels of information in terms of variety and scope.
3. an *Application of information loop* (R5) that results in an upward or downward impact on work pressure which has an effect on the level of documentation of incidents. The result is a stronger or weaker growth of explicit knowledge which, again, impacts the application of information. Indeed, referring to the above, we know that a broadening of information will result in more flexibility and hence in more IS capability.

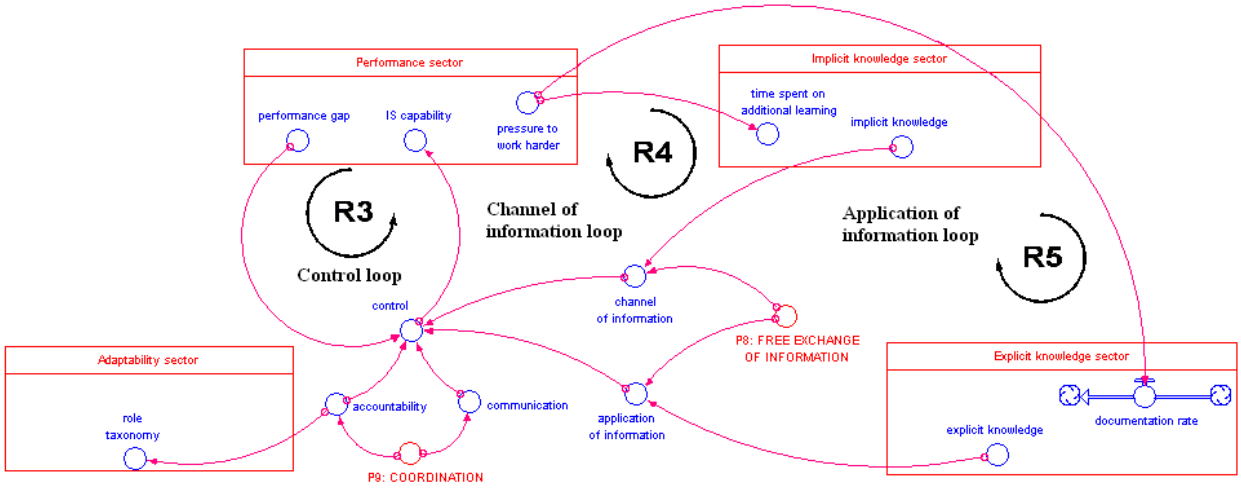

Figure 6 Control sector: Control Determinant

Third determinant of IS Capability: Implicit Knowledge

The implicit knowledge of the incident handlers is an important determinant of their ability to handle incidents with the IS and is represented by the total of their lessons learned (see Figure 7). The 'Lessons Learned' stock is increased by the Incident Management experience and additional learning, and is decreased by a constant memory loss rate. DERMIS design Premise P1 states that using the same IS is essential if incidents are to be handled successfully. Translated to our SD model, if the IS is used under as many circumstances as possible, than the Lessons Learned stock will increase with this experience, resulting in an increase in implicit knowledge and thus an increase in IS capability. The sixth reinforcing loop, the *learning loop* (R6), shows a side-effect of the pressure to

work harder to increase the solving speed. When the pressure to work harder increases, incident handlers must concentrate on solving the incidents quicker and have less attention to additional learning. This results in a decrease in the additional learning rate and so, combined with the same memory loss rate, in a lower degree of implicit knowledge.

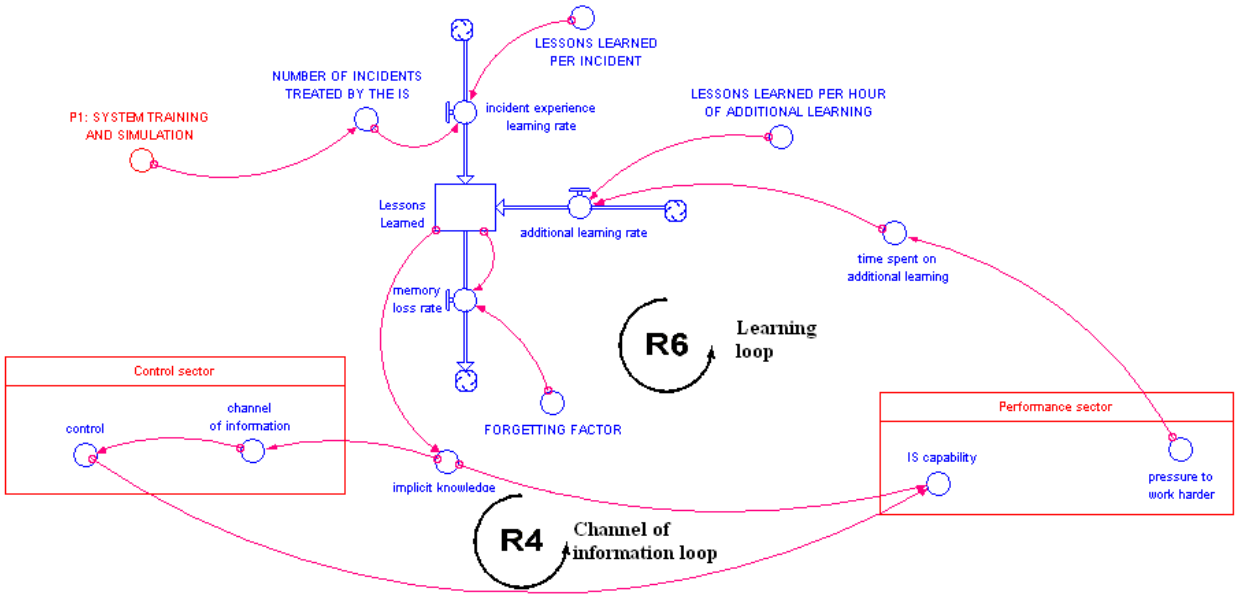

Figure 7 Implicit knowledge sector: Implicit Knowledge Determinant

Fourth determinant of IS Capability: Explicit Knowledge

The last determinant of IS capability is the degree of explicit knowledge (Figure 8). It is extremely important to document the incidents and the way they have been handled. If the documentation (and thus the explicit knowledge) is complete and up-to-date, it is easier to retrieve the way former incidents were handled, resulting in time-saving and avoiding the necessity to reinvent the wheel. The second side-effect of the pressure to work harder becomes visible in the seventh reinforcing loop, the *Documentation Loop* (R7): If the pressure increases, incident handlers will have less time to devote to documentation, resulting in a decrease in the proportion of time spent on documentation in relation to the time needed for proper documentation and so a decrease in the degree of explicit knowledge.

DERMIS design Premise P3 “Crisis Memory” stresses that learning and understanding what actually happened in incidents is extremely important for the performance of the Incident Management process. If this premise is complied with, the perceived importance of the documentation rises, resulting in more time spent on documentation. The “Cumulative Time Spent On Documentation” stock also increases when DERMIS design premise P7 “Information Validity and Timeliness” is satisfied, for incident handlers realize that it is critical to supply the best possible up-to-date information.

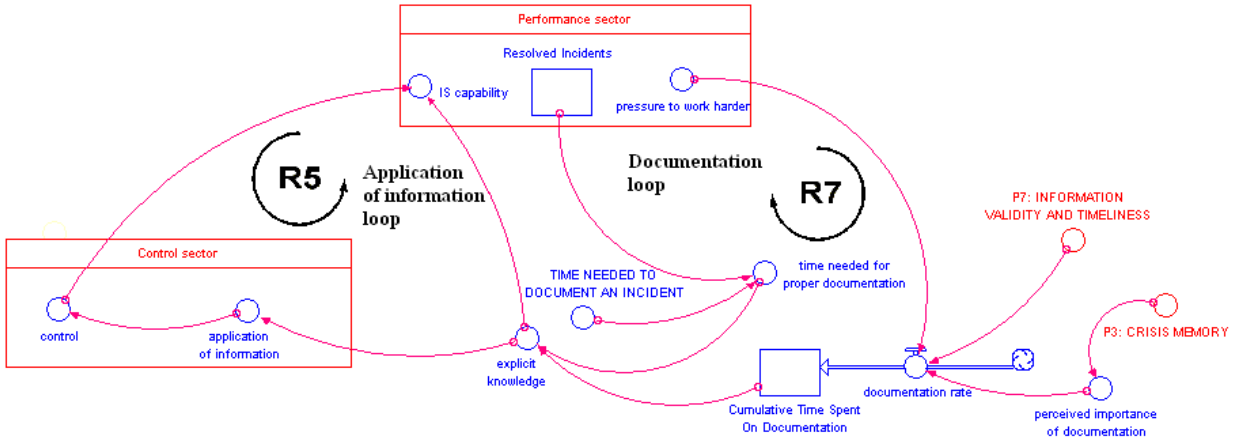

Figure 8 Explicit knowledge sector: Explicit Knowledge Determinant

CONCLUSION AND FUTURE RESEARCH

In this 'research in progress' paper, we have presented a System Dynamics model for the Incident Management process as influenced by the Capability of the supporting Emergency Response Information System, which we have in turn defined by means of the DERMIS design premises.

In the near future, we plan to validate our SD model with real Incident Management data obtained from the Incident Management process at a large organization where we are currently conducting a field study. We will also expand the currently developed model in such a way that it will allow for simulation. Such a simulation will allow for determining those factors and feedback loops that contribute most to IS Capability. The conclusions could serve as advice for the development of IS Design guidelines. For IS in general and ISCRAM in particular.

ACKNOWLEDGEMENTS

We would like to thank two anonymous reviewers for their constructive comments on a previous version of this paper. One of the authors' (Van de Walle) research is supported by the European Commission under the Sixth Framework Programme through a Marie Curie Intra-European Fellowship.

REFERENCES

1. Alavi, M. and D. Leidner. (2001) Knowledge management and Knowledge Management Systems, Conceptual Foundations and Research Issues. MIS Quarterly, Vol. 25, Issue 1, pp.107-136.
2. Boland, R. and Y. Yoo (2003) Sensemaking and Knowledge Management. In: Handbook on Knowledge Management 1, Knowledge Matters. Berlin Heidelberg, Springer Verlag. pp. 381-392.
3. Cannon, H. (1995) Dealing with the complexity paradox in business simulation developments. In: Business Simulation & Experiential Exercises, Vol. 25. pp. 96-102.
4. Central Computer & Telecommunications Agency (CCTA) (2000) Best Practice for Service Support. ITIL, The key to Managing IT Services. Norwich (UK), The Stationey Office, 298pp.
5. Kampfner, R. (1998) Dynamics and information processing in adaptive systems. Biosystems, Vol. 46, Issues 1-2, pp.153-162.
6. MacInnis, P. (2005) Creating a blueprint for IT professionalism. Computing Canada, Vol. 31, Issue 11, p18.

7. McLucas, A. (2003) Decision Making, Risk Management, Systems Thinking and Situation Awareness, Canberra, Argos Press, 232pp.
8. Nathan, M. (2004) How past becomes prologue. A sensemaking interpretation of the hindsight-foresight relationship given the circumstances of crisis. Futures, Vol. 36, pp. 181-199
9. Newman, D.and Nkei, B., Carreras, B., Dobson, I., Lynch, V.I. (2005) Risk Assessment in Complex Interacting Infrastructure Systems. In: Proceedings of the 38th Hawaii International Conference on System Sciences. 10pp.
10. Peppard, J. and Ward, J. (2004) Beyond strategic information systems, Towards an IS capability. The Journal of Strategic Information Systems, Vol. 13, Issue 2, pp.167-194.
11. Repenning, N. and Sterman, J. (2001) Nobody Ever Gets Cedit for Fixing Problems that Never Happened, Creating and Sustaining Process Improvement, California Management Review, Vol. 43, Issue 4, pp. 64-88.
12. Rudolph, J. and Repenning, N. (2002) Disaster Dynamics, Understanding the Role of Quantity in Organizational Collapse. Administrative Science Quarterly, Vol. 47, pp.1-30
13. Sawicka, A., Gonzalez, J. and Qian, Y. (2005) Managing CSIRT Capacity as a Renewable Resource Management Challenge. An Experimental Study. In: Proceedings of the 23rd System Dynamics Society Conference, Boston, MA, USA, July 17-21, 31p.
14. Snook, S. (2002). Friendly Fire. The Accidental Shootdown of US Black Hawks over Northern Iraq, Princeton, Princeton Universitary Press, 257p.
15. Staw, B, Sandelands, L. and Dutton, J. (1981) Threat-Rigidity Effects in Organizational Behavior, A Multilevel Analysis. Administrative Science Quarterly, Vol. 26, Issue 4, pp. 501-524.
16. Sutcliffe, K. and Vogus, T. (2003) Organizing For Resilience. In K.S. Cameron, J.E. Dutton, & R.E. Quinn (Eds.), Positive Organizational Scholarship, San Francisco, Berrett-Koehler, pp.94-110.
17. Turoff M., Chumer, M., Van de Walle, B., Xiang, Y. (2004) The Design of a Dynamic Emergency Response Management Information Systems. Journal of Information Technology Theory and Application (JITTA), Vol. 5, No. 4, pp.1-35.
18. Ward, J. and Peppard, J (2002) Strategic Planning for Information Systems. Third edition, Chichester (UK), John Wiley & Sons, 640p.
19. Weick, K. (1988) Enacted Sensemaking in Crisis Situations. Journal of Management Studies, Vol. 25, Issue 4, pp. 305-317.