The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0965-3562.htm

Business continuity planning methodology

John Lindström, Sören Samuelsson and Ann Hägerfors
Luleå University of Technology, Luleå, Sweden

Abstract

Purpose – The purpose of this paper is to present a multi-usable business continuity planning methodology. It comprises business continuity planning on the organizational and departmental levels.

Design/methodology/approach – The methodology has been developed, tested and confirmed in three comprehensive cases. Senior management, IT managers and employees in the three case organizations have participated in this action research effort during the development, implementation or training on business continuity plans and planning.

Findings – The methodology has been tested and confirmed, and is suitable for explaining business continuity planning to senior managements and employees in both public and private sector organizations.

Practical implications – The methodology description can be used for explaining the issues to senior managements and forms the foundation for a business continuity plan, which is part of an organization's IT- and information security program. It may also be used to explain business continuity planning to other staff in an organization. The methodology can also be used to model business continuity planning, as a basis for training planning, and as support in different training contexts to achieve individual and organizational learning on business continuity plans and activities.

Originality/value – The methodology of using a staircase or capability maturity model is a commonly used concept and can be adapted to any organization.

Keywords Business continuity, Contingency planning, Senior management, Training

Paper type Research paper

1. Introduction

The background and motivation for this paper is that during the planning for and development of business continuity plans as well as in training on business continuity planning at several corporations and government agencies, no good and simple way to explain the methodology of business continuity planning to the senior management (as well as to the rest of an organization) could be found. This was, however, of crucial importance for raising consciousness on the importance of senior management engagement in business continuity planning as well as on how to go about creating such a plan.

The business continuity plan is part of the strategic steering instruments for senior management (Lindström and Hägerfors, 2009), but often not cared for properly (Kajava *et al.*, 2006; Smith, 2004). Decisions on strategic IT- and information security, as defined in Lindström and Hägerfors (2009), where business continuity planning is included should not be conveniently delegated to only one member of senior management or to the IT-department or like. Owing to the growing importance of IT- and information security for most organizations, the strategic parts need to be integrated in the senior management agenda on a continuous basis in order to be maintained and cared for (Anttila *et al.*, 2004). Senior management (top management) should own and spend time

Disaster Prevention and Management
Vol. 19 No. 2, 2010
pp. 243-255

0965-3562
DOI 10.1108/09653561011038039

on the strategic parts of the business, as the strategic decisions affect the operational decisions in an organization at lower level if working in a top-down manner.

However, to get senior management to understand business continuity planning methodology, business continuity planning, and why they need to own and care for this continuous planning process – there is a need to explain it in a less abstract way (Kajava *et al.*, 2006; Smith, 2004) where it is possible to relate to something more familiar. It is also necessary to explain how the different elements of strategic IT- and information security are related and fit together in an organizational perspective (Lindström and Hägerfors, 2009).

There is a lot written about business continuity planning like NIST with Swanson *et al.* (2002), ISO/IEC 17799 (2005), the Swedish Emergency Management Agency's framework "Basic Level for Information Security" called BITS (2006), report from the Swedish Finance Inspection (2005), Lam (2002), Fallera (2004) partly, Roberts (2006), and Helms *et al.* (2006) on how to organize and develop business continuity planning and what to think about maintaining it. To work with or according to standards during business continuity planning is a good way to structure the work process, but there is also some criticism from Ma and Pearson (2005) and Sipponen (2007) concerning that organizations sometimes rely too much on the checklists provided.

Leveson has written numerous papers, for instance (Dulac and Leveson, 2004, 2005) together with Dulac on hazard analysis (mainly safety-oriented) used in the design process of complex systems to mitigate the hazards already during the design instead of adding them later on after a completed design. Johnson (2006) brings up the term "emerging properties" which represent according to him one of the most significant challenges for the engineering of complex systems. The "emerging properties" definition is disagreed on, but could be described as when users adopt products to support tasks that designers never intended (Johnson, 2006). This paper discusses these ideas in a business continuity planning context.

One of the important issues in business continuity planning is IT- and information security. Regarding integrating IT- and information security in the management of organizations, Anttila *et al.* (2004) discuss that information security is an integral part of modern business management systems to create a competitive advantage, requiring close co-operation between security experts and business executives. They also describe a variety of management-related issues taken from international standards that builds up a security program. They state that it is extremely important to understand information security issues in the context of business processes and that information security management is fully analogous to the management of other important areas like finance, quality, and business risks. They bring up that it is very important that senior management is interested and spend a lot of time on IT- and information security and that the area needs the same attention as all other important areas of a business. However, it is probably not likely that will happen (Kajava *et al.*, 2006) if senior management is to care for the whole security program. This paper continues to build on the work in (Anttila *et al.*, 2004) by introducing a model to explain business continuity planning methodology to senior managements.

Kajava *et al.* (2006) discuss that top managers often only have a superficial understanding of information security which may lead them to make decisions that are not conducive to raising the organization's security level. Also mentioned is that only 20 per cent of managers realized that information security is of strategic value to their

companies. They state that enhancing the information security awareness among all employees has been found necessary, but the key to success is to raise the awareness level of senior management – who often shies away from the training. They also together with Lempinen (2002) state the need to advance from a discussion on standards like ISO/IEC 17799 (2005) to a change in the culture. They also state that commitment from senior management to information security is of utmost importance to pave the way towards the information society, and recommend that a member of senior management should be responsible for coordination of the organization's information security policy. Further, they state that the key component of information security work is the viable support and engagement of senior management, by for instance participating in information security-related events.

Sipponen (2007) means that information security management standards focus on the existence of processes and not the content of what they are securing. Information security management standards like ISO/IEC 17799, GASPP and SSE-CMM which are widely used and advocated by researchers and practitioners have a limitation in that they focus on ensuring that security processes exist while being unconcerned about how these security processes can be accomplished in practice.

This paper continues to build on the work in (Kajava *et al.*, 2006) as the methodology introduced in this paper is used for explaining business continuity planning to senior managements. The intention is to raise awareness and understanding of these issues in order to improve the support and engagement from senior managements concerning business continuity and IT- and information security planning.

Grimaila (2004) discusses how to train students on strategic, tactical, and operational management of information security, also mentioning that later on in life security practitioners need technical, social and political skills (to be able to "sell" information security to senior management). Business continuity planning and disaster recovery planning are brought up as core issues. It is also stated that awareness and education are key to the success of a security program's overall success. Bazerman (2002) states that managers can make better decisions by accepting that uncertainty exists and learning to think systematically in risky environments. "After all, risk is not bad; it is simply unpredictable". Bazerman's observation is important and learning to deal with uncertainty and risks seems as important as learning how to minimize uncertainty.

Training in general is about helping people to learn by experience and to work more effectively. A good definition of what training is has been provided by Goldstein (1992): "Training is defined as the systematic acquisition of skills, rules, concepts, or attitudes that result in improved performance in another environment". A further discussion of training can be found in Goldstein (1992); Warren (1979); Molander (1990); Arkin (1994); Lierman (1994); Villegas (1996). Concerning content of training, Anderson (1994) emphasises that while training must continue to teach people things they do not know, it must also be about building on what is already known.

There are numerous ways of learning and dissemination of knowledge. To get a perspective as well as discussion about experiential learning, modelling, and tools (simulation/games) to support experiential learning, see Samuelsson (2002, 2006); Samuelsson and Hägerfors (2004). The important issue in this case is the connection between individual and organizational learning (Villegas, 1996; Samuelsson, 2002;

Baldwin and Ford, 1988; Senge, 1994) since the awareness raising and training aims at achieving organizational change. There is a need to adapt advanced training for each organization as well as clarifying that there is a responsibility among participants to enhance their learning. However, Summerville (1999) argues that it is unrealistic to expect teachers in all educational settings to alter educational environments in order to meet each student's educational needs, such as differences in cognitive style.

In a business continuity context – it is preferred not to learn from real experiences but rather from experiences when training. The reason for using training experiences is that a crisis management team should preferably be prepared to handle a crisis before it happens. Of course real experiences should be taken care of and used to improve the business continuity plan as well as the related training. However, Smith (2004) states that it might be better to use real experiences from other organizations or to try to separate the involved individuals from the situation context in which the individuals operate to avoid post-crisis blaming of individuals.

The understanding of the methodology to develop and maintain a business continuity plan is probably equally important of knowing how to use one, due to that the methodology makes an organization understand what maturity level they currently belong to and what is required to proceed further. Understanding the methodology and that business continuity planning is a continuous process – is of vital importance for successful business continuity planning.

2. Methodology

The business continuity planning methodology has been developed in three cases conducted during the last four years. Senior management, IT managers and employees in the three case organizations (both corporations and state agencies) have participated in this action research effort during the development, implementation or training on business continuity plans and planning.

In each of the three cases an action research approach has been utilized. Action research has been defined as:

> . . . a participatory, democratic process concerned with developing practical knowing in the pursuit of worthwhile human purposes, grounded in a participatory worldview which we believe is emerging at this historical moment. It seeks to bring together action and reflection, theory and practice, in participation with others, in the pursuit of practical solutions to issues of pressing concern to people, and more generally the flourishing of individual persons and their communities (Reason and Bradbury, 2001).

Characteristics of action research are that action researchers act in the studied situations, that action research involve two goals: solving the problem (the role of the consultant); and making a contribution to knowledge (the role of the researcher), that action research requires interaction and cooperation between researchers and the client personnel, and that action research can include all types of data-gathering methods (Gummesson, 2000). In this research the researcher has acted as an expert or consultant in the role of case leader being responsible for the cases that also have involved client personnel at the participating organizations.

The original development of the methodology started four years ago during development of business continuity plans for the first two cases. During the course of explaining business continuity planning new aspects was added to the original

methodology. Finally the methodology described below was tested and validated in the latest of the three cases.

First, a simple staircase was used to illustrate the need to improve by moving upwards on an organizational level. The department perspective was added in the second organization as it was realized that the maturity perspective was missing if not maintaining the current state. The possibility to fall down the ladder was also added. Further, in the last case, the arrows describing the situation severity to illustrate that an organization should able to handle more severe situations as better prepared were added.

That resulted in a graphic description of business continuity planning methodology used in the latest case. In this case a business continuity plan for a state agency was created from scratch to handing it over to the part of the organization that will continue to maintain and develop the plan including all steps of development, implementation and trainings.

Training and awareness raising were during the first two cases conducted for the employees directly involved in either the crisis management teams or the different recovery teams. During the last case, training and awareness raising was given to all employees in the organization with additional training for the crisis management teams, supporting specialists and recovery teams.

To learn about the effects from using the methodology when explaining business continuity planning, interviews were made with eight interviewees from the last case, where the methodology descriptions shown in section 3 were used.

3. Business continuity planning methodology

The methodology described uses an example of an organization comprising senior management and departments reporting directly to senior management. An organization organized in functions or divisions can easily adapt the way the departments are described to prepare.

The methodology description is intended to be used in organizations for explaining business continuity planning methodology to senior managements (and middle management). The description does not contain all steps and measures needed for business continuity planning, as it would then get too detailed. The description is intended to explain the business continuity planning methodology, and if more details are needed regarding all the steps – these are well described in for instance ISO/IEC 17799 (2005); Swedish Emergency Management Agency (2006); Lam (2002); Fallera (2004); Roberts (2006).

The Swedish Customs Service Stairway^{TM} model (2000)[1] and other capability maturity models (CMM) like SSE-CMM (2003), and CMMI (2007) are alike the model described in this paper maturity models that describe the path an organization should proceed to improve and continuously increase the maturity of the area of processes in focus. Lam (2002) has described an eight-step business continuity planning cycle which is a development and maintenance methodology.

In connection with business continuity planning and its methodology, Verstraeti (2004) brings up that most corporations today has become so lean that the question is if they are agile to handle disruptions in the corporate critical processes. Verstraeti introduces a lean/agility maturity model where the corporate management needs to adapt the management of the business processes and underlying information systems

to be able to react to change quickly and easily by hedging the risks. The advantage with using a staircase or capability maturity model is that it is a commonly used methodology concept and that it can be adapted to any organization.

An organization starts at the bottom of the staircase and intends to climb upwards according to the dashed arrow in Figure 1. The dotted arrows in Figure 1 are "situations", which are events that may develop into a crisis. A crisis is when an organization's critical processes are seriously affected or possibly if a very serious event affecting the organization has occurred. The model is mainly intended to handle situations related to critical processes. The length of the situations symbolizes increased severity – i.e. the higher up in the staircase, the more serious situations can be handled without going into a crisis. When having made certain business continuity measures, an organization climbs a step upwards at a time, and the organization gradually improves its ability to handle situations. When an organization has climbed one step, it will be able to cope with a situation that prior the measures taken probably would have developed into a crisis.

The more measures taken – the more steps are climbed – and the organization is able to handle increasingly serious situations within the organization in a controlled manner without the need to invoke crisis management and start up the business continuity plan.

On the other hand, if the business continuity measures taken are not maintained and updated, the organization will start to fall down the staircase and thus not be as agile as before to handle situations anymore. This is illustrated by the down pointing arrow to the left.

Figure 2 is a more detailed version of the model in Figure 1, laying out the methodology. The organizational perspective is on the left hand side and the departmental perspective is on the right hand side. The arrows on the sides are in the Figure 2 double directed, i.e. it is possible to go both upwards and downwards.

Below, the steps on the left hand side in Figure 2 are described:

(1) Senior management sets objectives and limitations for a business continuity plan using the business plan, organizational vision, strategy and objectives, and gets involved in the continuous process to develop and later on to maintain a business continuity plan.

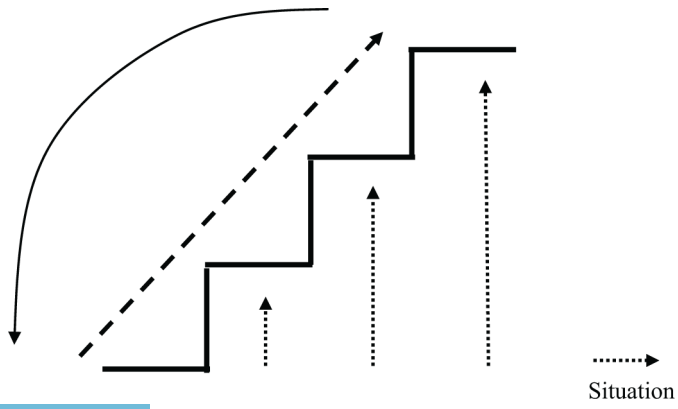

Figure 1.
High level "staircase" or capability maturity model

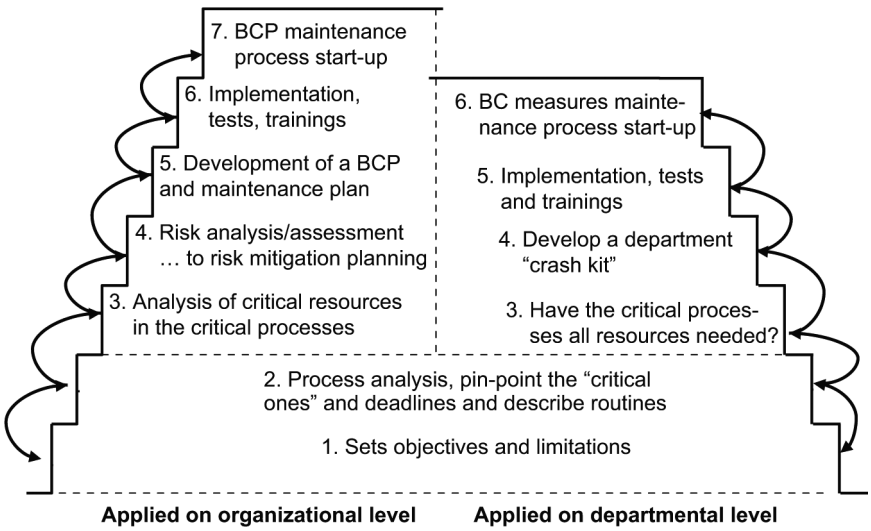

Figure 2.
"Staircase" methodology applied on organizational and department level

(2) Process analysis – analyze the organization's processes, improve them, and pin point the "critical ones". Find the hard deadlines in the processes and describe the routines in the processes starting with the critical ones.

(3) Analysis of critical resources in the critical processes, i.e. management personnel, personnel, IT-systems/tools used and supplier list, business partners, check that reserve routines exist and are described, mapping of ISO/IEC 17799 requirements on the critical IT-systems/tools etc.

(4) Risk analysis/assessment … to risk mitigation planning.

(5) Development of a business continuity plan and maintenance process/plan.

(6) Implementation, tests, trainings and practices.

(7) Business continuity planning maintenance process start-up. Now there is a business continuity plan to use and maintain.

The implementation spans that the organization starts to use the business continuity plan (including a crisis management organization) and handles the risks that are deemed necessary to mitigate, for instance an alternative work site might be needed to set up.

The departmental level, see on the right hand side in Figure 2, differs somewhat from the organizational level due to that it is here the majority of the business continuity measures should be implemented. The reason for this is that it is at the departments where the actual handling of situations occurs. Often multiple departments work together in processes, and the IT-department is in a majority of organizations involved in most situation mitigations:

(1) Senior management and department management set objectives and limitations for business continuity measures using the business plan broken down on a department level. Department management gets involved in the continuous process to develop and later on to maintain the business continuity measures.

(2) Process analysis – use the process maps made and pin-point the "critical ones". Add more process levels if more details are needed. Any hard deadlines? Describe the normal routines in the processes starting with the critical ones.

(3) Make sure the critical processes have all critical resources needed (i.e. management personnel, personnel, IT-systems/tools used and supplier list, business partners, all contact information needed, reserve routines exist and are described – any critical process should have one or more reserve routines for all steps, etc.).

(4) Develop a department "crash kit" containing all critical resources (including planning for usage of critical personnel if need to use an alternative site or go all-around-the-clock and department escalation/communications plan etc.).

(5) Implementation, tests, trainings and practices.

(6) Business continuity measures maintenance process start-up. Now the department has set up the business continuity measures needed and need to maintain them.

The departmental level business continuity measures are important to keep up to date as it is on this level most changes occur. To keep in mind is that the processes' routine instructions (normal and reserve routines) need to reach a level where in worst case a reserve with some support from someone with experience can perform the job needed. This is due to that in a crisis it is not likely that all ordinary personnel are available to perform their normal duties. The interaction with other departments in processes may also have an impact – if other departments introduce changes in their own processes.

A comparison between this model and methodology and Lam's (2002) cyclic model shows that both see business continuity planning as iterative processes. However, this model is less detailed and targets senior management primarily whereas Lam's cyclic model seems intended for a more general use among business continuity planners when actually creating a business continuity plan. Fallera (2004) describes partly what is needed regarding business continuity planning (however, using the terms risk management and disaster recovery planning) on a management level but does not introduce a model containing methodology which could be used during training. Roberts (2006) seems to focus on continuity planners creating a business continuity plan. As mentioned earlier, an advantage with using a staircase or capability maturity model is that it is a commonly used methodology concept and that it can be adapted to any organization.

The whole business continuity planning on the organizational and departmental levels can be seen as an iterative process, using the business plan as input with a business continuity plan or measures as the outcome.

4. Findings

During the last case the methodology was rated on a scale from 1.00 (bad) to 10.00 (excellent) and also commented on. The outcome of the rating was an average of 8.06, median value of 8.00 and a standard deviation of 2.06. As the standard deviation was quite large, and there also was information of the interviewees' professional background, it was checked if there was any difference if the interviewees had a

background from the private sector before entering the public one compared with those with only experience from the public sector.

Four interviewees had extensive experience from the private sector and four had only experience from the public sector. The comparison showed that the ones with private sector background rated the model with an average of 9.38, median value 10.00 and with a standard deviation of 1.25, and the ones with public sector background rated the model with an average of 6.75, median value of 7.25 and with a standard deviation of 1.94.

It seemed that the model was better for those with private sector background. Investigating why this was the case, it emerged that the interviewees with a public sector background felt that another additional example from their organization was needed in combination with the description to fully understand the methodology. As it seems like employees from the private sector are more aware/used to the need of business continuity planning, its terminology, and methodology compared to employees in the public sector, this may be a topic where further research on a larger scale could show if there really is a difference between private and public sector regarding this matter.

5. Discussion

Explanatory models are needed to educate, create an understanding and create a change in culture required (Kajava *et al.*, 2006; Lempinen, 2002) to be successful when implementing a business continuity planning process. The explanatory model that is used to explain business continuity planning methodology is quite general for those organizations that rely on information systems and an IT-infrastructure (i.e. critical resources) in the critical processes. However, a business continuity plan should be adapted specifically for the target organization.

A business continuity plan needs to work in practice and not only in theory. The objective for an organization ought to be to be able to solve all situations in a calm and structured way without the need to open up the business continuity plan, as it is known by heart.

Organizations sometimes rely too much on the checklists provided in existing standards. A business continuity plan is probably more useful if it is used as a general support tool to solve any kind of situation and not only as a guide for a set of predefined situations (although some specific situations could/should have checklists prepared – the number of specific situations may depend on the type of industry, laws and regulations, if toxic or radioactive substances etc. are handled). Those checklists for predefined situations need to be created during the business continuity planning process and kept updated in the following maintenance process. As Bazerman (2002) states that managers need to learn to think systematically in risky environments, it is probably as important as to learn how to minimize risks or uncertainty (which is much more common in management training).

To be able to reach this level, an organization needs to be mentally prepared that situations may occur at anytime, keep the business continuity plan maintenance process running, and educate, train and practice both internally and with external partners such as business partners, public organizations, suppliers and contractors with service level agreements (SLAs) etc.

Dulac and Leveson (2004, 2005) discuss hazard analysis (mainly safety oriented) used in the design process of complex system (where IT and information systems are comprised) to mitigate the hazards already during the design instead of adding them later on after a completed design. Business continuity planning strives to keep an organization to deliver the output from the critical processes during the mitigation of problems to get back to a normal situation again. If applying the ideas from Leveson and Dulac to try to design out the hazards from the critical work processes and the information systems used in these, it would probably be to expensive for most organizations to do it compared to using reserve routines or other information systems with overlapping functionality. The reason for this is that often information systems are bought as standard packages and the time and cost to adapt them is high.

However, the information systems are sometimes integrated or linked together very tightly to support the work processes. Johnson (2006) describes "emerging properties" as the phenomena appearing when users adopt products to support tasks that the designers of the system never intended. This is quite a problem from a business continuity perspective. If a complex of integrated information systems introduces possibilities that where not planned by the designers – it may be hard for those working with business continuity planning to find reserve routines or other information systems with overlapping functionality that could be used instead.

The work of Leveson, Dulac and Johnson does not perhaps directly impact the model for explaining business continuity planning methodology to senior management, but indirectly it could be a good idea to also mention to senior management during training that to try to "keep the work processes and supporting information systems as simple as possible" is a good idea as the work with business continuity planning get easier then (thus being part of the methodology).

6. Further research and use of the methodology

As it seems as employees from the private sector are more aware/used to the need of business continuity planning, its terminology, and methodology compared to employees in the public sector, this may be a topic where further research could show if there really is a difference between private and public sector regarding this matter.

It is important that the whole organization from top to bottom has the same understanding of both the methodology and the business continuity plan, not only to keep up the maturity level, but also as many members of an organization are involved during the planning process. Training and the use of simulators for crisis management using the business continuity plan is a good way to involve more members of an organization and also increase the awareness of that a crisis might occur. Experiential learning using simulations and games are good learning enhancers for experience-based learning. Training using business simulators for business continuity planning scenarios as well as directly for IT- and information security policy problems is an interesting topic for future research.

Further, the ideas of Leveson and Dulac on safety oriented hazard analysis used in the design of complex systems and Johnsons discussion on "emerging properties" as one important challenge for engineering of complex systems are interesting topics to explore in connection with continued development of the business continuity planning methodology.

Note

1. The Stairway model is extended with the new EU AEO model (Authorised Economic Operator) from end of 2007 – an organization with an AEO certificate is on level 4 or 5 in the Staircase, available at: www.tullverket.se/sokordao/a/authorisedeconomicoperatoraeo.4.7ebd8a201190f9e732f8000145. html

References

Anderson, G. (1994), "A proactive model for training needs analysis", *Journal of European Industrial Training*, Vol. 18 No. 3, pp. 23-8

Anttila, J., Kajava, J. and Varonen, R. (2004), "Balanced integration of information security into business management", *Proceedings of the 30th EUROMICRO' 04, IEEE*.

Arkin, A. (1994), "Computing the future means of training", *Personnel Management*, August, pp. 36-40.

Baldwin, T.T. and Ford, J.K. (1988), "Transfer training: a review and directions for future research", *Personnel Psychology*, Vol. 41, pp. 63-105.

Bazerman, M.H. (2002), *Judgement in Managerial Decision Making*, 5th ed., John Wiley, New York, NY.

CMMI (2007), Carnegie Mellon University, Pittsburgh, PA, available at: www.sei.cmu.edu/cmmi/

Dulac, N. and Leveson, N. (2004), "An approach to design for safety in complex systems", *Proceedings of the International Conference on System Engineering (INCOSE '04), Toulouse, June*.

Dulac, N. and Leveson, N. (2005), "Incorporating safety in early system architecture trade studies", *Proceedings of the International Conference of the System Safety Society (ISSC '05), San Diego, August*.

Fallera, P. (2004), "Disaster recovery planning – the best defense is a well managed offense", *Potentials, IEEE*, Vol. 22 No. 5, December.

Goldstein, I.L. (1992), *Training in Organizations: Needs Assessment, Development and Evaluation*, Brooks/Cole Publishing Co., Monterey, CA.

Grimaila, M.R. (2004), "Maximizing business information security's educational value", *IEEE Security and Privacy*, Vol. 2 No. 1, pp. 56-60.

Gummesson, E. (2000), *Qualitative Methods in Management Research*, 2nd ed., Sage, Thousand Oaks, CA.

Helms, R.W., van Oorschot, S., Herweijer, J. and Plas, M. (2006), "An integral IT continuity framework for undisrupted business operations", *Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES'06), IEEE*.

ISO/IEC 17799 (2005), *Information Technology – Security Techniques – Code of Practice for Information Security Management*.

Johnson, C.W. (2006), "What are emergent properties and how do they affect the engineering of complex systems?", *Reliability Engineering and System Safety*, Vol. 91 No. 12, pp. 1475-81.

Kajava, J., Varonen, R., Anttila, J., Savola, R. and Röning, J. (2006), "Senior executives' commitment to information security – from motivation to responsibility", *Proceedings of the International Conference on Computational Intelligence and Security, IEEE*.

Lam, W. (2002), "Ensuring business continuity", *IT Pro IEEE*, May/June.

Lempinen, H. (2002), *Security Model as a Part of the Strategy of a Private Hospital* (in Finnish), University of Oulu, Oulu.

Lierman, B. (1994), "How to develop a training simulation", *Training & Development*, February, pp. 50-2.

Lindström, J. and Hägerfors, A. (2009), "A model for explaining strategic IT- and information security to senior management", *International Journal of Public Information Systems*, Vol. 2009 No. 1.

Ma, Q. and Pearson, J.M. (2005), "ISO 17799: 'Best practices' in information security management?", *Communications of the Association for Information Systems*, Vol. 15, pp. 577-91.

Molander, C. (1990), *Organization Development*, Mulvie & McDougall.

Reason, P. and Bradbury, H. (Eds) (2001), *Handbook of Action Research: Participative Inquiry and Practice*, Sage Publications, London.

Roberts, W. (2006), "Business continuity planning for disasters is just good planning", *Proceedings of the Military Communications Conference (MILCOM 2006)*.

Samuelsson, S. (2002), "A study of teaching and learning environments for business games" (in Swedish), Licentiate thesis, Luleå University of Technology, Luleå.

Samuelsson, S. (2006), "IT-based business games for experimental learning – system structure and enablers" (in Swedish), doctoral thesis, Luleå University of Technology, Luleå.

Samuelsson, S. and Hägerfors, A. (2004), "Computer supported business games", *Proceedings of the Information System research Seminars in Scandinavia (IRIS 27)*.

Senge, P.M. (1994), *The Fifth Discipline Fieldbook. Strategies and Tools for Building a Learning Organization*, Currency Doubleday, New York, NY.

Sipponen, M. (2007), "Information security management standards: problems and solutions", *The DATA BASE for Advances in Information Systems*, Vol. 38 No. 1, February.

Smith, D. (2004), "For whom the bell tolls: imagining accidents and the development of crisis simulation in organizations", *Simulation & Gaming*, September, pp. 347-62.

SSE-CMM (2003), *Systems Security Engineering-Capability Maturity Model*. SSE-CMM Project, v 3.0 edition.

Summerville, J. (1999), "Role of awareness of cognitive style in hypermedia", *International Journal of Educational Technology*, Vol. 1 No. 1, July.

Swanson, M., Wohl, A., Pope, L., Gance, T., Hash, J. and Thomas, R. (2002), *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication, June, pp. 800-34.

Swedish Customs Services Stairway™ model (2000), available at: www.tullverket.se/sokordao/s/servicetrappan.4.5b2d990b116c8e66b0f800050.html

Swedish Emergency Management Agency (2006), "BITS – Basic Level for Information Security", available at: www.krisberedskapsmyndigheten.se/templates/Publication____1143.aspx, 2006:1

Swedish Finance Inspection (2005), "Status of the finance industry's crisis management 2005:3", report from 17-March-2005 (in Swedish), Dnr 05-1249-601.

Verstraeti, C. (2004), "Planning for the unexpected", *IEEE Manufacturing Engineer*, June/July.

Villegas, J. (1996), "Simulation supported industrial training from an organisational learning perspective", doctoral thesis, Department of Computer and Information Science, Linköping.

Warren, M. (1979), *Traning for Results: A System Approach to the Development of Human Resources in Industry*, 2nd ed., Addison-Wesley, Glen View, IL.

About the authors

John Lindström is a member of the information security research group at Luleå University of Technology. He works in industry, currently as VP Client Service and Support at Mobizoft. He has worked for many years with product development, and technical- and management consulting in the IT/information security business. John Lindström is the corresponding author and can be contacted at: John.lindstrom@cdt.ltu.se

Sören Samuelsson is an assistant professor in Computer and Systems Sciences at Luleå University of Technology. He has held the positions of Dean for a number of years and is Head teacher of the division of Computer and Systems Sciences. In the division, he researches within the areas of computer-based simulations/games and information security.

Ann Hägerfors is a full professor in Computer and Systems Sciences at Luleå University of Technology. She has held several leading positions, e.g. as Dean of the philosophical faculty, and is currently head of the division of Computer and Systems Sciences. In the division, she has built a viable research environment in information and knowledge management concerning foremost long-term digital preservation, but also management of information security and e-learning.