DECISION SUPPORT TECHNOLOGY TO SUPPORT RISK ANALYSIS AND DISASTER RECOVERY PLAN FORMULATION

Towards IT and Business Continuity

Anne-Francoise RUTKOWSKI, Willem VAN GROENENDAAL and Bartel VAN DE WALLE
Department of Information Systems and Management, Tilburg University, Tilburg, the Netherlands
Email { a.rutkowski,W.J.H.vGroenendaal, bartel}uvt.nl

Jan POL
Philips Medical Systems, Best, the Netherlands
Email: j.pol@philips.com

Keywords: Business Continuity; ICT Recovery Planning; Group Support Systems; Risk Analysis

Abstract: The paper presents a four-phase action research project that was (and still is) conducted at the department of Information Management Customer Support and Operations (IM\CS&O) of a large multi-national company. The department is in charge of ICT-service continuity and has to produce ICT recovery plans that are integrated with the organization's overall Business Continuity plan. Interviews, Group Support System (GSS) technologies as well as a risk survey have been used to gather information and identify risks and threats. A systematic quantitative classification, measuring the impact of loss of ICT services on the company's business processes in terms of cost and risk will allow in the near future to utilize an economic decision model to prioritize the core activities of training and implementation of a recovery disaster plan. The research has made clear to the involved protagonists the necessity to share information, to develop awareness, and to formulate a shared recovery disaster plan to ensure ICT/business continuity and/or recovery when ICT disruptions occurs..

1. INTRODUCTION

Organizations have become more and more dependent on Information Systems and Technology, further referred to as ICT, to run their business processes, manage workflows, and communicate. The loss of the availability of a critical Information System (IS) can disrupt business continuity and harm the organization's critical business processes, and with it its reputation and financial prosperity. Business continuity is intrinsically related to the businesses' Information Technology (IT) and IS services continuity.

Ensuring continuity of ICT within an effective timeframe, following a disruption or disaster, to maintain or get business processes running is essential for the survival of many organizations (Doughty, 2002; Suh and Han, 2003). Identifying the risks that may cause a disruption in ICT continuity is essential for an organization. Even more crucial is to build and plan effective and efficient recovery scenarios that facilitate the timely recovery of the ICT facilities. For a recovery plan to be beneficial to an organization requires understanding the structure and the organization of both the business processes and the related ICT units. Indeed, research in the field of risk management has shown that the interaction between different types of risks can amplify the damage to a business process and generate a crisis for the organization concerned (Williams et al., 1997). Business disasters and crisis are focusing events that trigger attention to a problem and its solution, and that are generally accompanied by drawing negative attention to the firm and the underlying problem revealed by the event (Baumgartner and Jones, 1993). In other words, focusing on risk management often reveals the weak parts of an organization, but do not receive sufficient attention in most companies.

This paper presents a research in the spirit of action research that was conducted at a large organization for the department of Information

Management Customer Support and Operations (IM\CS&O). Although a business on its own, the organization studied is part of a larger organization, with which it shares some ICT services. The IM\CS&O department is, however, in charge of ICT service continuity and has to produce an ICT recovery plan, which will be an integral part of the total organization's overall Business Continuity plan. To guarantee a high level of ICT-service continuity, IM\CS&O commissioned an investigation into the threats to its ICT services in relation to its business processes, and into the possibilities to prevent and/or mitigate these threats. The services provided by the IM\CS&O department affect the continuity of four main business processes. This investigation deals with on site ICT disruptions, not with the systems shared with others. The effect of disruption of shared services will be analyzed, but the contingency plan for disruption is formulated at a higher organizational level. Disaster recovery procedures, as well as back-up systems, have to be available to both the ICT and the business employees in order to either help prevent it or to mitigate the effects. To identify and reduce the impact of ICT disasters on business continuity it is crucial to conduct an effective risk analysis and formulate disaster recovery scenarios and plans.

The purpose of this article is not to present in detail the conclusions of the research for the organization, which is not concluded yet, but rather to describe the methodological steps that were taken to develop awareness on the necessity to build disaster recovery scenarios and plans, and on the information gathering process for the construction of the scenarios and plans. The following sections present the different phases of our research, and we conclude by offering some recommendations for the systematic development of risk analysis and disaster recovery plan in organizations.

2. BACKGROUND

Business continuity is intrinsically related to ICT services continuity. Because ICT systems have become more and more integrated, an organization's flexibility to deal with discontinuity has nowadays diminished considerably. As was stated above the disruption of any critical ICT service can seriously harm business continuity. This is beyond the loss of production only, since it also harms the business' reputation and thus its long term financial prosperity.

As was stated by most business managers, a brief disruption in ICT services can be put into profit by reducing the backlog in administrative paperwork. The consequences of the disruption are then limited since they are time dependent. If the problem persists, however, the consequences become more severe. The professionals whose work is strongly computer dependent, such as production, logistics, and in our case service to customers all over the world, will however be affected also and it is unclear how time critical these processes are. Precautionary measures and restoration processes have to be identified and organized in order to develop efficient disaster recovery plans. An ICT disaster does not only cause immediate problems, but can harm the business process in the long-term also. Since the organization has only a limited number of internationally operating competitors, a serious disruption will harm its reputation as a reliable high tech company and can lead to loss in market share.

Financial consequences are numerous when business continuity is partially or fully interrupted by ICT failures e.g., loss of customer orders, loss of vital data, man-hours, or too long disruptions of machinery in place with customers to name just a few. The cost in terms of man-hours lost is fairly easy to estimate, the loss in reputation is more difficult to establish. Identifying all possible threats and their financial consequences is a lifetime job, if not impossible. Outside threats, such as a plane crash or an earthquake, are always possible, but difficult to estimate. The detection of ICT threats to the key business processes is somewhat easier. Mathematical modeling techniques, research of historical data from within or outside the company, expert advice are some of the possibilities available to determine threats, and if realized the duration of its effect. Opinions vary, however, on the matter of what in this respect expertise is and who the experts are.

In the research presented here we consider senior managers and staff members experts with respect to ICT failure and its consequences; they are considered the key-players in the organization. These persons are therefore to be consulted in order to gather information on threats and the related risks for the relation between ICT and business processes. This information is used with a concise description of the business processes and its relations to the ICT systems. All this in order to built efficient recovery disaster plans in case of crisis situation. Note that a threat can be external, in which case we can prepare to limit the consequences, or internal in which case we can try to prevent it, that is limit the risk and limit the consequences.

In this paper a threat is defined as an event that, if it occurs, will harm the business financially. The risk associated with a threat is the probability that the threat realizes for a particular time interval. The seriousness of a threat is normally related to its duration when it occurs. For example a power outage of a few minutes for Customer Services is a possible threat, but the financial consequences of this risk can normally be neglected. A power outage of several days on the other hand will be harmful.

We define a crisis as a decision situation with serious financial consequences that is characterized by an element of surprise (sudden realization of threat) and limited time to take appropriate action. The quality of the decision taken is then highly dependent on the social perception of the person or group of persons in charge. Social sciences have shown that the probability of defective group decision-making, for instance group think, is higher when the situation is very stressful and the group is too cohesive and socially isolated. The participants involved in the decision are cognitively overloaded and the group fails to adequately determine their objectives and alternatives, fail to explore all the options and also fail to assess the risks associated with the group's decision itself (Janis, 1982). Further, the consequences of a crisis may affect stakeholders around the globe. It is the absence of recovering strategies that transform a crisis situation in a disaster.

Decision Support System (DSS) and Group Decision Support System (GDSS) methods and technologies have been developed over the last two decades. The software package GroupSystem was the first GDSS technology that supported the technique of anonymous brainstorming and is recognized as reducing the groupthinking effect. Decision Explorer and the SODA methodology have been used widely in risk management projects and are recognized to be efficient to develop shared meanings amongst the protagonists of a group confronted with a crisis situation (Ackermann And Eden, 1983). Cognitive Mapping is a technique that has been developed over a long period of time and through its application has demonstrated its use for Operational Research and Management Science working on a variety of tasks. These tasks include providing help with structuring messy or complex data for problem solving, assisting the interview process by increasing understanding and generating agendas, and by managing large amounts of qualitative data from documents. While cognitive mapping is often carried out with individuals on a one to one basis, it can be used with groups to support them in problem solving as well (see Ackerman and Eden, 2003).

In order to have a better grasp on the different risks and their inter-relations that can be a potential threat to the organization, communication and coordination should be supported to avoid group think or internal focus and to favor the development of shared meaning between the different units of the organization. Once the threats of ICT failure have been identified along with the associated risks, a systematic quantitative analysis in money terms of their impacts on company business processes is feasible. For this we are developing an economic decision model based on traditional financial risk analysis. This will allow us to design crisis prevention policies to mitigate risks and to prioritize, from a financial perspective, scenarios for disaster recovery through training activities.

3. METHOD

We outline our research method in the following sections.

3.1 Phase I : Cognitive map building

At the start of the project, interviews were conducted with 20 senior managers of the organization using a strict open question interview protocol based on the free-association method.. The goal of the interviews was to gather the views of ICT and business on continuity, this to better understand the gaps between both communities. Following the interviews a content grid analysis was done; next the not-knowing approach (Gergen, 1998) was used as a baseline theory to build three wild cognitive maps, constructed by an outside observer instead of the protagonists. This research was done previously as part of the action research.

The two resulting maps, shown in Figures 1 and 2, represent the overall perception of the ICT and business managers on ICT/Business continuity respectively. Figure 1 presents the view of the business managers on continuity and indicates that the numerous consequences of a threat are well known in terms of customer relationship and cost but business managers grossly underestimate the possible threats of ICT service failures. The map shows that for many of the facts (another name for a threat) indicated and of their consequences, the business group knows hardly any solutions, other than "try to catch up with time", "write things done on paper and enter later" or "call the ICT helpdesk". Figure 2 presents the view of the ICT managers on continuity and clearly shows that the business

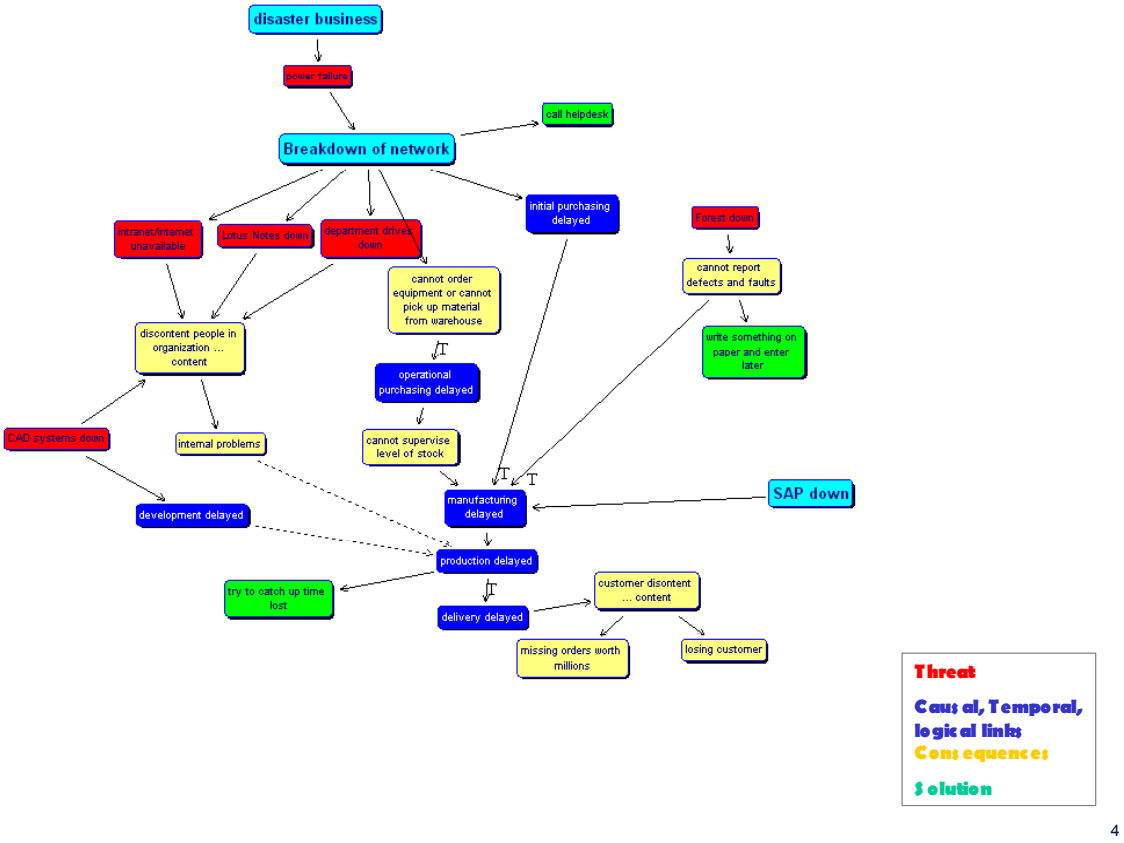

Figure 1 Business managers' view on business continuity

solution "call IT helpdesk" is not applicable, because in case of an ICT failure the "helpdesk is unavailable". ICT thinks in terms ICT solutions, but grossly underestimates the impact on customers and business processes. Still, interesting to note is that "think of an emergency solution" can hardly be called an efficient solution to the problem.

When comparing it to the map representing the ICT view it is striking that most solutions brought forward by the business managers are actually not applicable. Business thinks in terms of time (indicated with the 'T'-links in the map), while ICT services thinks mainly in terms of logical links or/and their consequences (indicated with the '&'-links in the map). This latter view is typically technology driven. It is interesting that a simple combination of both maps already gives a clear representation of the causal, temporal, and logical links between threats and their consequences as well as the unknown links to both protagonists.

These cognitive maps were then used during a presentation to underline the gap between the two groups, but also to emphasize the need for more awareness and collaboration to tackle this complex problem. The combined map was also used to reinforce shared meanings between both professional groups that belong to the same corporation, share a common interest in ICT/business continuity, but seem to lack basic understanding of each others work. Having both groups of participants communicating and made aware of the situation was a first important step to their commitment to the following two workshops.

3.2 Phase II: Decision Support Systems

3.2.1 Session I: Brainstorming using a GSS (GroupSystem)

The eight participants involved in a 3-hours brainstorming group session were managers in charge of Information Management, Development, and Sales. This session was organized to brainstorm on critical business processes and their dependencies on ICT.

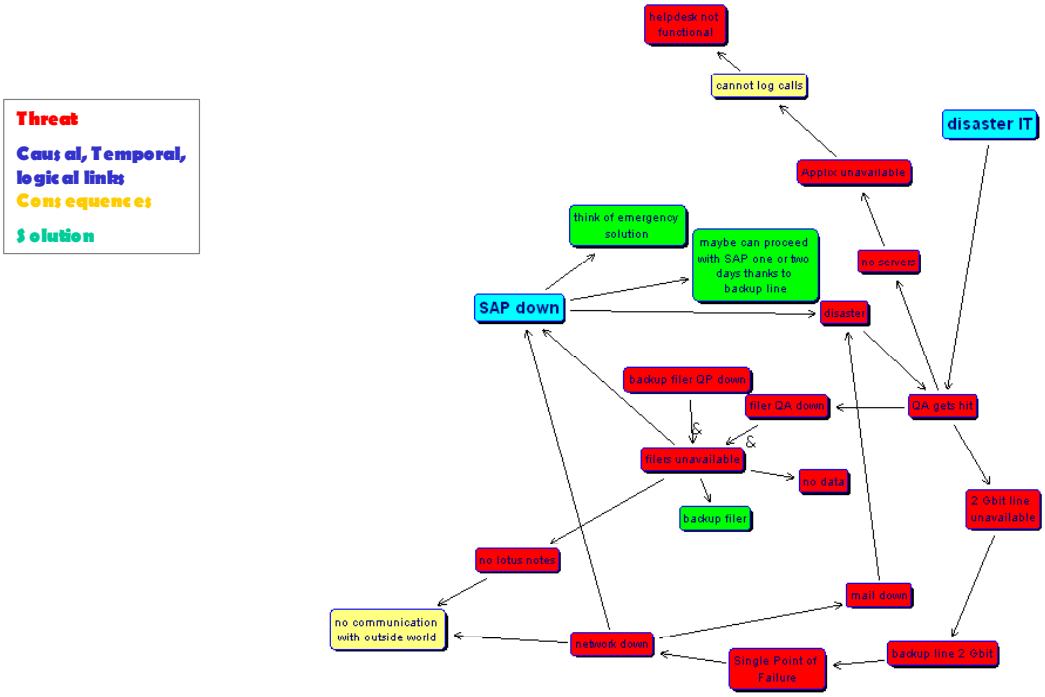

Figure 2 IT managers's view on business continuity.

The electronic agenda consisted of two main categorizers. The first categorizer was related to the depedencies on ICT within the organization.

Questions on topics, such as employee dependencies on information technologies and services to perform their task, the effect of ICT failure on the employee's work and productivity within and between departments, as well as preventive/recovery measures and processes for ICT failure were used as support to brainstorm on this categorizer.

The second categorizer allowed the participants to brainstorm on the quantitative classification of threats of the ICT service continuity, including cost associated to failure, reputation, and share values.

The third categorizer supported a brainstorming session on the probability of a threath occurring, its risk, and the method that should be used to have a realistic view on this occurrence (e.g., historical data analysis versus experts opinions).

The results of the vote sessions on the 15 named major threats were rated on 10-point scale (1 is lowest impact / likelihood and 10 is highest impact / likelihood) indicated that threats such as worm/virus attack (external cause) as well as power outage (internal cause) were interesting to consider in the next phase of the research due to a balance impact/likelihood.

3.2.2 Session II: Shared Meaning and Recovery Plan using a GDSS (Decision Explorer)

Another group of ten senior business and ICT managers was invited 4 weeks later to participate in the cognitive mapping session. The participants were randomly attributed an ICT disaster scenario that described either a worm/virus attack or a power outage within the organization; both scenarios had been recognized during the first session as two

major ICT threats. In the first phase of the 4-hours session, the 10 participants built their individual cognitive maps representing the best recovery plan strategy to the disaster presented. The participants should focus on the consequences of the disaster on the business line continuity and recovery measures to be taken.

Most participants built their individual map in about 1 hour. We then formed 2 sub-groups of 5 participants to discuss their individual maps and recovery plan strategies in order to construct a combined cognitive map that will aggregate the individual view. Within 2 hours the participants had reached consensus and developed two combined maps for each of the IT disaster cases that provide an interesting structure to build recovery disaster plans.

4. DISCUSSION

So far this research has made clear to the protagonists involved the necessity to share information in order to become aware of ICT threats, the associated risks and the financial consequences. The cognitive maps show that the business and ICT managers had surprisingly different views on ICT threats and their effects on business. Neither group is actually aware of the potential problems. The business managers know to some extend the expected cost of an ICT service failure, but have no real feeling for what actually may go wrong is this respect. The ICT managers on the other hand know in detail what ICT systems are running, but have insufficient knowledge of the business consequences.

Currently all links between the business processes and the ICT systems are identified and used to determine potential threats. Simultaneously the associated risks are estimated as well as the expected time related costs. These will be used to get the business and ICT managers at the same awareness level. If all parties agree, the results will be used to estimate the expected financial cost per occurrence. Also potential dependencies between threats will be established. With this information the IM\CS&O department can then develop risk mitigation plans and recovery scenarios.

Risk management is a topic that concerns many companies. As stated in the introduction of the paper however, focusing on risk management often reveals the weak parts of an organization and does not receive sufficient attention in most companies. From a behavioral and social perspective humans do not show the natural drive to focus on failure (Bower, 1981) and have the tendency to attribute failure to external causes and factors out of their control. Professional knowledge gaps and misunderstanding amongst different groups reduces the perspective of the participants. Awareness supported by the approach we present appears to be a first interesting step towards obtaining shared meanings.

The research has made clear to the involved protagonists the necessity to share information, to develop awareness, and to formulate a shared disaster recovery plan to ensure ICT/business continuity and/or recovery when ICT disruptions occur. The research process that involved the use of GSS and DSS was crucial to start the communication process between both professional communities of practice, and to reduce the gap between antagonists who often held complementary views. Indeed, the research in Phase III brought interesting results on the table under the form of integrated cognitive maps that, more than the combination of perspectives on IT/business continuity, activated and supported by the brainstorming session as well as the mapping session, opened the mind of the protagonists towards shared understanding of the importance of crisis management.

As the methodology describes in the paper combines knowledge elicitation with traditional risk analysis, some questions on the validity remain. Moreover, for obvious reasons the details and the results of the sessions cannot be presented. The research is still in progress and conclusions are difficult to draw in terms of methodological validity. Nevertheless, to the authors the internal validity of the research appears to be strong , but the question remains whether the method can used in other companies.

REFERENCES

Doughty, K. (2002). Business continuity: A Business Survival Strategy, *Information Systems Control Journal, 1*, 28-36.

Pol, J (2000). Process description IT Service Continuity Management, Philips internal report.

Suh, B., and Han, I. (2003). The risk analysis based on a business model, *Information and Management,* 1-9.

Williams, T.M., Ackermann, F., and Eden, C. (1997). Project Risk: Systemicity, cause mapping and a scenario approach. In Kahkonen, K. and Artto, K.A. (eds), *Managing Risks in Projects*: 343-352. London: E&FN spon.