The International Emergency Management Society
9th Annual Conference Proceedings
University of Waterloo, Canada, May 14-17, 2002

ORGANIZATIONS, LEARNING AND RISK MANAGEMENT

Jean-Luc WYBO

Ecole des Mines de Paris[1]

Keywords : Risk management, crisis management, organizational learning, organizational silienrece

Abstract

The management of risk, alerts and crises in the industry is a complex task, which is achieved by a large number of stakeholders. This paper presents the advantages associated with the development of organizational learning to analyze alerts and crises, which provides a better sharing of knowledge about identification of weaknesses and strengths, and a deeper involvement of people in risk management.

Introduction

The objectives of risk management are not only to suppress or to reduce hazardous events, but also to be able to react in the best ways when risk develops into accident or crisis. To reach these objectives, organizations establish means and strategies for prevention and mitigation.

If the system (technological or not) may be risky and the nature of these risks are well known, then it is possible to build strategies aiming at protecting this system against perturbations that may be at the origin of dangerous situations and crisis.

Prevention corresponds to several kinds of actions:

- Analyze potentially hazardous events and situations and study their origins and consequences.
- Analyze the system vulnerabilities: components that may be damaged, persons that may be wounded and functions of the organization that may be disturbed.
- Install technical devices or procedures to suppress hazardous events or make them harmless.
- Set up an organization that favors the integration of the notion of risk at all levels.

People achieve the management of incidents, accidents and crises through two complementary ways: application of procedures and improvisation.

If the incidental situation has been anticipated and analyzed, for instance during the system design or following a similar incident, its management will follow an incident management procedure and will be facilitated by appropriate protection devices and organization models, which are called barriers or defenses.

If the situation escapes from this framework, either because the incident was not considered and never occurred before, or because defenses have not functioned, then we turn to a type of management based on experience and improvisation of people. These people will do their best to bring the system back into a known and stable state, while limiting damage and disaster extent.

[1] Ecole des Mines de Paris – Pôle cindyniques, BP 207, F-06904 Sophia-Antipolis (France) – http://www.cindy.ensmp.fr

There is an unlimited number of organization types and combinations of actions that put an end to a crisis situation, and during these situations, one may often observe the emergence of leaders and interesting organization models. The different kinds of knowledge that are used or built during the management of these situations constitute an important wealth for organizations and companies, but they are often tacit and poorly shared among people.

> *The actors involved in safety system failures are frequently the primary, sometimes the sole, source of information about what happened and why. The capacity to learn from accidents and develop preventive measures therefore depends on the ability to elicit information.* [Mc Donald 1997]

Developing this knowledge, sharing it and improving the image of people who own it are, along with prevention, the most important ways of increasing the resistance of organizations to hazardous situations.

Complexity of the problem

In the last decades, a substantial improvement in technology reliability and risk prevention has been observed, but in parallel, a steady increase of system complexity tends to create new kinds of risks.

> *The role of the human being in complex systems is essential: he must achieve programmed and complex operations, but also supervise the system as a whole. In many cases, his job goes beyond simple compliance to procedures because their only application is not enough to get the production. Moreover, if it were the case, people would be replaced by automatic devices. Quite often, he must check the relevance of the procedure in the real context of the task and, in the eventuality of a gap, he must change procedure, complete prescriptions, or even invent new organization schemes to reach the goal, despite perturbations, while respecting safety requirements.* [Translated from Leplat 1990]

This complexity is often linked to the extension of technology and automatic devices that control the system, but it results also from the increase in the number of stakeholders and relations binding them. In the same way, the development of outsourcing, which contributes to the increase of productivity, may also bring a loss of tacit knowledge belonging to key people that contribute to the organization resilience, especially if these staff categories have a high turnover ratio.

Even if a part of this complexity can be identified and allow the setting up of reliable organization models and transparent flows of information, it also promotes the emergence of drifts, differences between people and dilution of responsibilities, which are key risk factors.

Debriefing incidents and accidents is becoming de facto one of the few ways to identify what we call “traces of complexity”, that is to say to enlighten, through detailed analysis of events and decisions, the behavior of technical, human and organizational subsystems when facing unexpected situations.

The human being, the organization and the resilience

When events or conditions occur that may turn into alerts or crises, there are simultaneously strong constraints, uncertainties on the development of the situation, and a need for a structure of organization. This structure is a landmark in the unknown, an obstacle to chaos. Which are the key factors that promote the setting up of an order, an organizational structure for the response to the alert or the crisis?

As early as the activation of an alert, by analogy with crystals growing, one or several "germs" will play the role of support or guide for the development of the structure, but they will rapidly become invisible and give room to an aggregation process that will generally only keep main directions from the initial germ. We call this "germ" the *kernel* of the organizational structure.

But this kernel is insufficient, as a source of energy is also required: the set of constraints that exert on people belonging to the different groups involved in the situation, which push them to participate in the organizational structure of emergency management and which allows its development and adaptation to the context.

In the case of an organization confronted by the management of an alert or a crisis, factors that participate in the setting up of an organizational structure will be the pressure of events, the extension of the alert, the motivation of people or their willingness to limit consequences. But who plays the role of kernel?

Two kinds of germs can be observed: people and action plans. In the first case, there are one or several leaders, whose role in the organization, charisma or reputation will attract people and form the initial germ.

In the second case, there is an action plan that is known well enough (sometimes more by its name than by its exact content) to be used by a first group of people as a reference, to initiate a structure following its indications.

In both cases (leader or plan), it can be observed that the complexity of crisis situations moves rapidly away from the hypothesis of the plan or the first leader's indications. "*Procedure is weak when confronted by urgency*" [translated from De Coninck 1995]. The situation then moves to a process of evolution and developing of the organizational structure, which will develop not only from the kernel, but also and mainly from the influences and constraints of the context (dangerousness, dissemination of products, media impact, etc.).

We use the term resilience to qualify the ability of organizations to resist dangerous situations with the minimum of damage. In the domain of risk management, the resilience of a system is built up in two phases:

- At the design stage, by promoting the design of a safe system, able to resist expected hazards and be provided with efficient barriers.
- During the life span of the system, by the analysis of incidents, of their management by staff and of the behavior of barriers, in order to assess weaknesses as well as resources that have provided solutions, and to learn lessons from these analyses.

When a system (company, municipality, etc.) is confronted by a crisis, a small group of people will take the responsibility of its management, either because it corresponds to their duties, or because they feel entrusted with this mission. To identify this network of people, which constitutes what we call the "resilience kernel" of the system, it is necessary to analyze examples of alert or crisis management and to identify the parties who have played key roles.

In most cases, organizations demonstrate efficiency and resistance to stress, events and time. It is not by chance, but rather because they follow a general scheme, based on the availability of a kernel (leader or plan) and on the existence of constraints and stress around this kernel. If these constraints go beyond a given threshold, which corresponds for us to the individual or collective acceptability of risk, then a structure (or a sub-structure) will grow around this kernel. This structure of organization is a sort of buffer zone that distributes constraints by relying on these germs. The goal is to shoulder constraints while protecting the system against damage. This buffer zone may concern actions, information management or grading the problems to solve.

By this way, each incident enlightens in the general architecture of the organization, a subset of people who have been involved and their relations among themselves and with the outside world, whenever they belong to the organization or they are opinion relays. The analysis of the different networks that have "emerged" during incidents, alerts and crisis management reveals what we call "pockets of resilience", which constitute the strengths of the system, but also its weaknesses, when these organization schemes have not been able to efficiently manage the situations.

> *The level of reliability of an organized system depends on the capacity of its parties to develop cleverness clues needed to achieve informal settings in order to continuously correct and amend a set of structurally incomplete rules and devices* [translated from Bourrier 2001[a]]

Among the benefits of debriefing and analysis of alerts and crisis management unfolding, this identification of the strengths of the system that must be promoted and its weaknesses that need to be corrected, is probably one of the most promising. It provides knowledge about the behavior of the system beyond its limits and it allows the identification of key people, information flows and resources on which the system may rely to anticipate, prepare and manage hazardous situations.

The contributions of organizational learning to knowledge

Knowledge imbedded in experience of individuals is difficult to grasp because it is spread throughout the organization and it is often tacit among groups. Moreover, it can only be revealed at the time of "problems" that are often badly identified by the hierarchy and the other groups, as a consequence of an organizational culture based on the sanction of errors.

This set of knowledge, often informal, tacit and acquired through years of practice, failures and successes, constitutes individual experiences of people. But this wealth of the institution is fragile. It assists in confronting difficulties and adversity but it may vanish if the organization is not aware of it, if the owners of this knowledge, what we call the "resilience providers," are not rewarded for it, and if it is not transmitted and shared among people, hierarchies and generations.

Setting up and developing an organizational learning scheme to make this knowledge visible and formalized is crucial. But it also creates a progress dynamics based on three principles: respect of individuals; trust in their ability to manage unexpected situations; and dissemination of information. It is also a way to reinforce the feeling of belonging to the structure of the system, which is a key factor for motivating and encouraging commitment in the development of a safety culture within the institution.

> *The definition of safety culture tries to bind the sphere of individual behavior (attitudes) and human errors, objects of predilection until the eighties, to the sphere of organization, structures and social behavior, objects that were not so much tackled until now* [translated from Bourrier 2001[b]]

Recurrent incidents are signs pointing to dysfunction and should be studied carefully. It is usual to limit their analysis to the search for technical factors that will be fixed or human failures that will be sanctioned. This kind of strategy turns out to have a limited efficiency and the frequency of incidents stays at a level which cannot be lowered any further.

The introduction of more refined debriefing methods may reveal structural factors that are the roots of these incidents and by that contribute to provide more efficient solutions.

> *Organizational learning requires that event analysis traces the causal factors and determinants of an event both further back into the past, and further up the chain of management control.* [Hale 1997]

Inside a group of people, organizational learning also results in the creation of communication and sharing of knowledge among individuals, whatever their missions or level in the hierarchy are.

> *The reliability of learning of an organization is if it develops common understandings of its experience and makes its interpretation public, stable and shared.* [March 1991]

This kind of communication gives opportunities to anyone to raise the standing of his own expertise and to learn from others: "management told us the reasons why"; "operators told us the way how".

Conclusion

The main objective of the debriefing process is to understand what happened and to find ways to avoid the repetition of accidents and to limit their consequences, using the lessons learned from the analysis of incidents and crises. Enlarging this perspective to set up a real organizational learning scheme sets the path to new goals that participate in the development of a risk culture among organizations.

The experience gained by the people is, with its successes and failures, an invaluable source of improvement [Wybo 2001[b]]. Incidents, quasi-accidents and crises may become, beyond simple debriefing sessions, opportunities to reinforce the trust bindings among people, contribute to promote their skills and provide a better knowledge of the system.

The management of incidents and crises is always a matter of exceptional events in deteriorated situations. Setting up a risk culture based on a global approach needs to take into account the complexity and, notably, to master its three main aspects: technical, human and organizational.

Based on the notions that have been presented in this paper, a methodology for debriefing and organizational learning is currently under development within an interest group composed of academics, companies and public bodies [REXAO]. This methodology is applied to different kinds of hazards: natural, technological and food-related.

Références

[Mc Donald 1997] Mac Donald N. (1997), in *After the event*, Hale, Wilpert, Freitag Eds., Pergamon, p 98

[Leplat 1990] Leplat J. & G de Tersac, (1990), in *les facteurs humains de la fiabilité*, éditions Octarés, p 11

[Wybo 2001[a]] Wybo J.L., Colardelle C., Poulossier M.P., Cauchois D., *A methodology to share experiences in incident management*, TIEMS conference, Oslo, June 2001

[de Coninck 1995] De Coninck F., (1995), in *travail intégré, société éclatée*, PUF, p 69

[Bourrier 2001[a]] Bourrier M. & H Laroche, in *risques, erreurs et défaillances*, publications de la MSH – Alpes, 2001, p 18

[Bourrier 2001[b]] Bourrier M. & H Laroche, (2001), in *risques, erreurs et défaillances*, publications de la MSH – Alpes, p 21

[Hale 1997] Hale A., (1997), in *After the event*, Hale, Wilpert, Freitag Eds., Pergamon, p 9

[March 1991] March J.G., L S Sproull and M Tamuz, (1991), *Learning from samples of one or fewer*. Organisation Science, 2(1), pp. 7

[Wybo 2001[b]] Wybo J.L. (2001), *Risky Business*, TOMORROW, N°3, Volume XI, June, pp 72-73

[REXAO] Groupement REXAO®. French interest group for debriefing and organizational learning (Retour d'Expérience et Apprentissage Organisationnel). http://www.rexao.org

Author Biography

Dr. Jean-Luc Wybo graduated in engineering from the Institute for applied sciences in Lyon and received a Master degree and a Ph.D. from the University of Nice. He is the Director of a research laboratory in risk management (Pôle Cindyniques) at Ecole des Mines de Paris and the Executive Editor of IJEM (International Journal of Emergency Management, Inderscience Ltd.).