Knowledge Management in an Age of Terrorism

Denise Johnson McManus
Assistant Professor of Information Systems, Exxon-Wayne Calloway Faculty Fellow, Wayne Calloway School of Business and Accountancy,
Wake Forest University, North Carolina, Tel: (336) 758-6174, Fax: (336) 758-6133, mcmanusd@wfu.edu

Charles A. Snyder
Woodruff Professor, Department of Management, Auburn University, Alabama
Tel: (334) 844-6515, Fax: (334) 844-5159, Snyder@business.auburn.edu

ABSTRACT

As the horrific events of September 11, 2001 in New York City, Washington, DC, and rural Pennsylvania unfolded, the first thoughts of most were likely for the victims of terror on such a huge scale. In the aftermath of the tragedy and destruction, many survivors had to turn to restoring businesses. Much was written about disaster recovery and business continuity planning as people struggled to regain the essential systems that underlie the modern organization. One aspect of this restoration that has typically been ignored is that of organizational memory management—a crucial part of Knowledge Management (KM). The importance of knowledge as a critical resource continues to gain recognition in the business world. This paper discusses the need for KM programs in order to cope with large scale disasters such as the World Trade Center attacks.

INTRODUCTION

Business continuity planning is often equated with external forces, such as natural disasters that present the risk of power disruption, building destruction, or worse (McManus & Carr, 2000). Less obvious is the risk inherent with a terrorist attack as devastating as the horrific events experienced by the United States on September 11, 2001. Risk is inherent in any organization, in any operation, in any situation where the goal is continuity.

An essential component of any sound Information Resources Management program is that of Business Continuity Planning or, in a more limited sense, Disaster Recovery Planning. These programs are emplaced to ensure that a business can continue to operate after a disaster. From an information technology perspective, the plans deal with restoring capability so that essential IT supported functions can be carried out. An important part of the recovery planning should be on the KM aspects that enable the systems to function. What are these aspects? What are the specific tasks that managers need to perform? How should managers address the KM tasks?

As stated by Dickerson, (2001), "In the coming days and weeks, businesses that lost employees in the attack are faced with realities of rebuilding business infrastructure to serve their customers amid the bottomless grieving for their colleagues. The loss of so many people means a catastrophic loss of intellectual capital." Therefore, even companies that have a good disaster recovery plan are struggling to implement the plan. While the total cost of damage to a company's equipment and facilities can easily be determined, intangible damage, such as the cost of downtime and the loss of intellectual capital are difficult to measure. Not only are companies faced with the loss of employees and loss of the business infrastructure, but also they are struggling with the rebuilding efforts due to lack of available company employees that can implement the plan. This solidifies the necessity to capture relevant knowledge that can be engaged during such catastrophic disasters as experience on September 11, 2001.

KM ASPECTS OF CONTINUITY PLANNING

Information technology managers have long advocated certain practices that make a business capable of restoring IT-based aspects of the business in disaster situations. Some of the most basic practices are backup, especially of critical applications. However, most disaster recovery plans that rely on conventional backup, outdated testing, narrow redundancy, etc. are woefully inadequate to comprehensively cover enterprise needs (Grygo, et al., 2001). With catastrophic disasters such as massive terrorist attacks, there is a huge human dimension in addition to the technical one. In some cases, the majority of the human resource may be lost in addition to the destruction of IT and

facilities. As Kearns (2001) stated, "it is not pleasant to contemplate, but what would your company do in the event that you and your entire department were wiped out?"

In an interview (Scannell, 2001), the head of IBM's disaster recovery center, Ted Gordon, stated that the basic disaster recovery plan was insufficient when the whole fabric of how the business operated was disrupted, rather than just getting computers back up and running. He said that, "Every company has to take stock of exactly how they do business, where it is most critical for them to keep that part of the business running, and what the processes are that support that…technology is not as big a risk as is the way we use technology to do business—it is the emphasis on the people, and our dependency on them, and how we choose to operate."

Companies must conduct risk assessment and manage the risk potential from all aspects of the company, i.e., personnel, technology. In the traditional disaster recovery plan, it was the responsibility of management to determine where unexpected and undesired consequences were likely to occur. The assessment was often focused on interruption of technology, process, or procedures. "The technological inability to communicate with customers and suppliers is devastating, which can prevent the company from staying in business. By detecting and recognizing risks, the result of adverse consequences will be less catastrophic" (McManus & Carr, 2000).

Comprehensive plans are designed to eliminate unnecessary decision making immediately following the disaster. This plan is only effective if the appropriate personnel are available to invoke the actions necessary to continue the business. The companies in the World Trade Center have experienced immediate problems from the terrorist attack, and will continue to experience difficulty for months, even years, and potentially may never recovery, because of the tremendous loss of intellectual capital.

Few firms have been so deeply and irrevocably devastated by the World Trade Center attack as KBW. In all, 67 of the firm's 172 New York-based employees died or are still missing. They accounted for nearly a third of KBW's 224 employees. In a stroke, the firm lost more than 400 years of professional experience and much of its leadership. Gone are five of nine board members, including KBW's directors of equity trading, bonds, and research, along with its most prominent and influential financial analysts. Those missing or dead were responsible for 40% of KBW's annual revenues, which reached $125 million last year. In addition to the human loss, the firm lost its headquarters and every shred of paper documentation that existed there (Byrne, 2001).

Many companies in the World Trade Center may have the ability to recover their technological losses quickly, however, not their intel-

---

lectual losses. In an interview with Howard W. Lutnick, a Cantor Fitzgerald Securities executive, he indicated that 68% of the intellectual assets of the company were lost in the tragedy. "The government bond trader had almost its entire New York staff wiped out on September 11" (Powell, 2001, p. 68). The company did not lose the critical data of the company, however, they did lose customer contact personnel, which will ultimately affect their supply chain management and CRM capabilities. It is apparent that the knowledge of the personnel of Cantor Fitzgerald Securities is a necessity to stay in business.

"Nothing can compare to the enormity of our loss of life," said Mr. Lutnick. "This tragic event has taken from us over one third of our employees (approximately 700), including half of our senior leadership. However, what we have learned from this horrendous act is that it is impossible, to destroy the spirit of our family and together we are forging ahead. We will remain the market leader with the foremost electronic trading platform in the world and in doing so honor the integrity of those employees, executives, family and friends we have lost" (Business Wire, 2001).

Although valuable data was stored in various applications, the employees with the knowledge of creating and using this information were killed in the attack and their knowledge died with them. Therefore, these examples indicate the necessity to store the data in a data warehouse, and manage the knowledge for future use. In an effort to replace the personnel, the company will encounter tremendous risk that includes the inability of the new employees to perform at the appropriate level, as well as, the risk of a start-up company stealing the business.

"Risk International's Mr. Wellman advised employers to spread staffers around and to 'minimize decision-making' to protect against catastrophes. Businesses that had all or most of their workforce in a single location violated a fundamental risk management principle, 'concentration of risk'" (Bradford, 2001, p. 21). How can survivors restore the firm's presence and ability to do business? "In a disaster, companies may be able to get the IT side up, but what about the rest of the company? What about management and production?" (Kovar, 2001, p. 71). One measure that managers need to address is that of harvesting the crucial knowledge of their best performers and preserving it. This should be a priority undertaking, as it may prove vital for survival in an era where terrorism poses new risks.

KM TASKS

Knowledge management has been a popular concept for several years; however, there are many definitions and controversies about the scope, content, and implementations still clouding the issues. In this regard, we believe that the scope and content may be clarified by delineation of KM tasks that are important for business continuity planning. Consequently, we list tasks that are relevant within this context.

Since managers are interested in capturing relevant knowledge about the key processes of their firms, it is now apparent that this should be part of the strategic goals of the company (Snyder, Wilson, & McManus, 2000). An organization's knowledge base and continuity plan needs to contain relevant (expert) knowledge that can be made available during a disaster. Peter Drucker (1993) stated in his book *Post Capitalist Society*, "The basic economic resource is no longer capital, nor natural resources. It is and will be knowledge." Managers are trying to understand what this means as they move their companies and information technology departments from strategies of data management, to information management to knowledge management. Organizations are now striving to establish knowledge management systems to assist in the dynamic business environment.

Knowledge management is the utilization of "the collective knowledge, experience and competencies available internally and externally to the organization whenever and wherever they are required" (Fearnley & Horder, 1997). We believe that knowledge is similar to potential energy in providing the basic competence to perform. A manager's major concern should be centered on the knowledge required to perform the organization's critical processes and tasks. Thus, our

focus is on the management of the corporate memory that is required for superior performance of those critical processes. This becomes even more important as the world's force engage in war activities and the human knowledge bases leave the organization.

To appreciate the problem with expertise retention, consider the dilemma that suddenly arises when highly valued employees leave the organization unexpectedly, as experienced by many companies on September 11. You want to retain that person's expertise; generally viewed as his or her knowledge. (Snyder, Wilson & McManus, 2000).

Corporate Memory Management is an integrated set of processes whereby the hidden insights from top performers are converted into specific, actionable know-how that is able to be transferred to thousands of employees via software (Snyder &Wilson, 1998). The process follows a sort of life-cycle approach (Snyder, Wilson & McManus, 2000). The parts of the process are:

Focus

The first step is to determine the existing explicit knowledge and implicit knowledge that is needed for the focal process. What are the know-how content priorities for this process? Then a formal project plan must be created to capture the information. This capturing process maintains the brain of the organization regardless of downsizing, attrition, or resignation of employees.

Find

Another one of the initiating steps involves finding top performing people and their critical activities. The top performers will be identified as a way to determine the source of critical actions. The nature of the person that is being sought and the output of that person's activities create knowledge as opposed to a simple action.

Elicit

Once identified, an understanding of these activities will be elicited from the key individuals. The activities of the top performers are educed and logically mapped in the knowledge harvesting process. KM must uncover the rules of decision within the activities of key performers.

Organize

The knowledge must be arranged in a coherent or systematic form. This procedure of structuring the knowledge into orderly and functional processes allows anyone in the organization to retrieve the necessary information quickly and efficiently. It is this inherent method that allows the organization's knowledge to be carried forward for future use of various applications within the company.

Package

The determination of how to properly package the knowledge so that it can be available when and where needed is a necessity. We must assess the best packaging form, e.g., an Electronic Performance Support System (EPSS). This process collects and preserves information or data on a particular subject within the organization. This is a non-trivial process because the application will have to be expertly structured to glean knowledge from the action of the user and ignore everyday data and information. These knowledge processes are recorded in a database that is accessible through a software package. Software can be used by anyone, increasing the organization's ability to make effective use of all harvested know-how.

Share

Sharing brings different aspects to the value and use of knowledge and will likely lead to the seeking and capturing of other knowledge and uses of previous and new knowledge not formerly considered. This captured knowledge can be distributed throughout the organization to individuals or groups that may require this relevant information. Throughout this sharing process, a corporate repository is developed where tangible "intellectual capital" of an organization can be captured and exchanged. This sharing phase allows individuals to track

activities while significantly increasing efficiency and effectiveness of existing groupware for any organization.

Apply

The purpose of a KM system is to allow people other than the key players to use the same decisions rules. Once these decision rules have been elicited and captured, they are only of value if we have a way to apply the newly gained knowledge. It is the employees of the firm that may request or seek assistance, employment, or admission of a specific task. By creating these applications through the knowledge harvesting process, these employees can seek that assistance from the database of knowledge that has be gained and stored from the experts of the organization.

Evaluate

Evaluation must be performed in order to determine the effectiveness of the applications. Appraisal of the resulting captured knowledge will occur during its application and sharing. In sharing the knowledge, it will be evaluated, a process that should be continuous so that the total database can be kept up-to-date, relevant and as small as possible. The organization needs to evaluate its learning systems and their contribution to useful knowledge. At the most basic level, learning should be evaluated by assessing the impact on individual performance.

Adapt

The KM system must incorporate the ability to adapt to new knowledge so that it can be refreshed. To maintain this core asset, knowledge, software is utilized to record the knowledge and activities of the company experts. By instantly recording all input information generated during the learning sessions, these processes increase the organization's ability to make effective use of all harvested know-how. Therefore, when a crisis occurs, the organization's knowledge can be shared with others. This sharing process allows for a quick recovery. The combination of these harvesting processes can significantly reduce time and result in improved thinking and decision making when a company is faced with a disaster.

A few case studies were used by Frappaolo and Wilson (2000) to illustrate the application of the approach. One case is of particular interest in the present context. This case is titled "Before A Key Employee Walks Out the Door." In this case, the firm was forewarned of the imminent departure of one of its key individuals. The firm recognized the importance of capturing his intimate knowledge of a critical process and proceeded to work through the parts of the Knowledge Harvesting process cited above. This is the sort of procedure that all firms need to go through before there is a known loss of knowledge if they are to build survival capabilities.

A MANAGER'S KM CKECKLIST

Companies are already thinking about IT lessons. They "will most likely reconsider centralizing key personnel at a single office-one company lost its entire disaster recovery team of nine people in the attack" (Wagner, 2001). Using some of the steps of Knowledge Harvesting, Inc. model as a basis, we have a series of actions for managers. One of the first tasks involves simply identifying the organization's key or critical processes. We would suggest that these processes be evaluated and ranked along a criticality scale in order to determine the areas for priority focus. A checklist can provide a normative model for managers.
1. Identify Key Organizational Processes
2. Rank-order with Most Critical Processes First
3. Assess organizational Readiness (From: Assessing Readiness, 1999)
   a. Determine knowledge orientation
   b. Assess Climate for KM
   c. Assess Culture
   d. Determine the Degree to Which Daily Operations Support Change
   e. Assess Information Architecture Ability to Support Change
   f. Determine Leadership Support for Change
   g. Determine the Scope and Magnitude of Change
4. Develop KM Plan
5. Select a Proof of Concept Process Project

   a. Employ a Proven Methodology
   b. Select a Doable Project
6. Implement Proof of Concept Project
7. Evaluate Proof of Concept Project
8. Extend KM Implementation to Priority processes
9. Ensure Integration and Update is Ongoing

These steps can assist managers in their efforts to harvest and preserve essential knowledge surrounding the organization's key processes. The checklist is a suggested model for managers to follow in adding an essential KM element in their business continuity plans. Only by doing this, can firms ensure that they can recover from unexpected disasters such as large-scale terrorism.

CONCLUSIONS

The disastrous affects of the events that occurred on September 11, 2001 will drive companies not only to consider the importance of traditional disaster recovery plans, but also to incorporate a knowledge management component that may have been overlooked in the past. The loss of intellectual capital has virtually crippled some companies, with no recovery possible. In the last ten years, a major disaster has been reported somewhere in the United States as well as the world, every year. The size of the disaster is not the determining factor of staying in business; it is a comprehensive business continuity plan that will determine the success of most companies. Firms must go farther than building a disaster recovery plan in the face of new threats. They need a comprehensive business continuity plan that includes the possibility of massive loss of knowledge. This plan must address organizational memory management. The technology infrastructure can be replaced, the physical facilities can be rebuilt, but it may be impossible to recover the loss of expertise unless there has been a concerted effort to harvest the knowledge and have it packaged so that the essence of the experts' implicit knowledge is preserved.

REFERENCES

Bradford, M. (September 24, 2001). Attacks put focus on crisis plans. *Business Insurance*, 39, 18-22.

Byrne, J. (October 8, 2001). How much loss can a firm take? *Business Week*, 3752, 68.

Business Wire (October 4, 2001), eSpeed's Chairman Discusses the Company's Business.

Dickerson, C. (September 21, 2001). Boundless generosity. *InfoWorld*, 25.

Drucker, P. *Post-Capitalist Society*. New York: Harper & Collins, 1993.

Fearnley, P. and Horder, M. (1997). What is Knowledge Management? Knowledge Management in the Oil & Gas Industry. *London Conference Proceedings Notes*.

Grygo, E., Prencipe, L., Schwartz, E., Scannell, E.,and Krill, P. (September 17, 2001). IT recovery efforts forge ahead. *Infoworld*, 38,17.

Kearns, D. (September 24, 2001). Disaster recovery: Are you ready? *Network World*, 39, 22-23.

Kovar, J. (September 10, 2001), When disaster strikes. *The Newsweekly for Builders of Technology Solutions*, 962, 70-77.

McManus, D. J., and Carr, H. H. "Risk and the Need for Disaster Planning." *Information Systems Management Journal*, 1-01-55: June, 1999, p. 1-7.

Powell, B. (Oct. 1, 2001). New world order: Battered but unbroken. *Fortune*, 6, 68-80.

Scannell, E (September 19, 2001). Boss of IBM's disaster recovery center tells what he learned from last week's crisis. www2.infoworld.com/articles/hn/xml.

Snyder, C. A. & Wilson, L. T. (1998). Technology Advances Supporting Electronic Performance Support Systems, pp. 1-6.

Snyder, C.A., Wilson, L. T. & McManus, D.J. "Corporate Memory Management: A Knowledge Management Process Model." *International Journal of Technology Management*, Spring, 2000.

Wagner, M. (September 24, 2001). Disaster's Aftermath – IT Scrambles to Restore Order – World Trade Center tenants use lessons from 1993 bombing, quickly switch over to backup systems. *Internetweek*, 879, p. 15.

Related Content

A Multimodal Sentiment Analysis Method Integrating Multi-Layer Attention Interaction and Multi-Feature Enhancement
Shengfeng Xieand Jingwei Li (2024). *International Journal of Information Technologies and Systems Approach (pp. 1-20).*
www.irma-international.org/article/a-multimodal-sentiment-analysis-method-integrating-multi-layer-attention-interaction-and-multi-feature-enhancement/335940

Building and Use of a LOM Ontology
Ghebghoub Ouafia, Abel Marie-Hélène, Moulin Claudeand Leblanc Adeline (2010). *Ontology Theory, Management and Design: Advanced Tools and Models (pp. 162-178).*
www.irma-international.org/chapter/building-use-lom-ontology/42889

The Role of Emerging Information Technologies for Supporting Supply Chain Management
Zlatko Nedelkoand Vojko Potocan (2018). *Encyclopedia of Information Science and Technology, Fourth Edition (pp. 5559-5569).*
www.irma-international.org/chapter/the-role-of-emerging-information-technologies-for-supporting-supply-chain-management/184257

E-Commerce Model Oriented to Cloud Computing and Internet of Things Technology
Guanghai Tangand Hui Zeng (2021). *International Journal of Information Technologies and Systems Approach (pp. 84-98).*
www.irma-international.org/article/e-commerce-model-oriented-to-cloud-computing-and-internet-of-things-technology/278712

Machine Learning-Assisted Diagnosis Model for Chronic Obstructive Pulmonary Disease
Yongfu Yu, Nannan Du, Zhongteng Zhang, Weihong Huangand Min Li (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-22).*
www.irma-international.org/article/machine-learning-assisted-diagnosis-model-for-chronic-obstructive-pulmonary-disease/324760