International Journal of Business and Management
www.ccsenet.org/journal.html
Vol. 4, No. 1
January 2009

Strategic Utilization of IT for Corporate Crisis Management: the Empirical Study on Textile and Automotive Suppliers Sectors

Muammer Zerenler
Department of Marketing
University of Selcuk
Konya 42079, Turkey
E-mail: muammerz@hotmail.com

Mete Sezgin
Program of Tourism and Hotel Management
University of Selcuk
Konya 42079, Turkey
E-mail: metesezgin@hotmail.com

Selcuk Burak Hasiloglu (Corresponding author)
Department of Marketing
University of Pamukkale-
Denizli 20070, Turkey
E-mail: selcukburak@hasiloglu.com

Abstract

This paper reports the findings of a survey on the use of Information Technology (IT) in crisis management in textile and automotive suppliers industries in Turkey. The survey was sent to 114 Turkish companies with 50 employees or more, resulting in a response rate of 46 %. Statistical analysis of the result demonstrate that although the development of crisis management plans leads to a higher awareness of the company risks, it is especially the creation of a crisis management team that leads to a higher degree of actions taken, for instance training or simulations. Moreover, this study demonstrates that the level of IT use in crisis management is predominantly related to the presence of a member in the crisis management team with an IT background.

Keywords: Crisis management, IT, Textile, Automotive

1. Introduction

Global competition has brought about changes that are characterized by product proliferation with shorter and uncertain life cycles, innovative process technologies, and customers who simultaneously demand quick response, lower costs, and greater customization. Companies must cope effectively with continuous and unexpected changes in order to become competitive. The ability to respond quickly and effectively (time-based competition) and to satisfy customer needs has become a distinctive characteristic of competitiveness for many manufacturing companies.

A crisis is a situation faced by an individual, a group or an organization, which they are unable to cope with, by the use of normal routine procedures and, in which stress is created by sudden change (Booth, 1993). Various authors like Fink (1986) also describe crisis as a period of sudden change during which a totally new system is formed; stressing on the fact that the meaning of crisis does not only cover risk, uncertainty, threat, conflict, accident, and instability but also covers opportunity.

Management of a major crisis requires prevention, planning, testing, evaluation and maintenance to mitigate and minimize the consequences. The process used by a company can determine the outcome for those affected, including employees, community and the company. A crisis is any natural, accidental or intentional event that severely impacts people, property, and/or the environment. Effects might include fatalities, disabling injuries, significant destruction or

contamination, jeopardizing the organization's reputation or products, or threatening a company's continued existence. The consequences are independent of company size, quality of management, industry or location.

Technology and ever changing threats challenge the preparation needed to manage situations that may affect an organization's future. Minimizing risk by application of process safety management tools and security systems is an important component of an overall plan.

2. Strategic utilization of information technologies

Nowadays, the business environment is characterized by great uncertainty and variability. In this environment, information technology (IT) has proved to be an important strategic ingredient for the creation of competitive advantage. In the new era of production, strategic priorities rather than a cost contained focus have proved to be important for competition, namely: quality, dependability, flexibility, customer service, after sale service, supply chain management, etc. IT proved to be vital for successful competition as it can facilitate the attainment of these strategic targets.

Information Technology (IT) has emerged as an essential element in developing countries such as Turkey in supporting the need for regular, real-time, and dependable information in business and industry (Eze, & Mohammad, 2000). The successful use of IT depends on the technology itself and the level of expertise of the individual using the technology. The impact of IT on user productivity and user satisfaction is said to be an indicator of the success of computer utilization (Davis, 1989). To study the nature and extent of IT utilization, research in computer utilization and acceptance and how the technology contributes to a firm's competitiveness in a developing country environment was undertaken.

As information technology and information systems today are embedded in all organizational levels and activities, a growing research and development effort has emerged in recent years that focuses on the design, development, use and evaluation of information systems that can help organizations prepare for, and respond to, a crisis (Turoff et al., 2004). For example, information systems have been used to understand the possible relationships among threats an organization is facing (Van de Walle & Rutkowski, 2006). While corporate crisis planning and preparedness in general is the setting of this research paper, a particular point of interest addressed here are the particular motivations, if any, of managers to use IT in the different stages of crisis management in their company.

Implicit in crises of varying scopes and proportions are communication and information needs that can be addressed by today's information and communication technologies. In a comprehensive review, Turoff et al. (2004) systematically develop a set of general and supporting design principles and specifications for a Dynamic Emergency Response Management Information System (DERMIS) by identifying design premises resulting in part from the use of "Emergency Management Information System and Reference Index" (EMISARI), a pioneering emergency management information system built by Turoff and used in the 1970s at the US Presidential Office for Emergency Preparedness, and in part based on a comprehensive literature review.

3. Corporate crisis management

Crisis management is generally considered a strategic management activity aiming to prevent or minimize the impact of a crisis for the organization. Crisis management is a dynamic and systematic process encompassing the phases of prevention and mitigation, preparedness, response and recovery (Fink, 1986; Preble, 1997; Pauchant et al., 1992). The initial phase of prevention and mitigation typically involves a threat or vulnerability analysis, leading to an identified list of risks that may provoke a crisis upon their materialization. Identified risks may be eliminated (for instance by installing a software patch for some identified system vulnerability), diverted (for instance by buying Service Level Agreements), or accepted and prepared for (e.g. by installing duplicate systems at a remote site). These activities are often referred to as risk management, which in general leads to a risk management plan. A crisis management plan on the other hand addresses the response phase of the crisis, and outlines the measures, strategies and procedures to be taken, and the responsibilities of those involved. A crisis management team is usually activated to prepare for coordinating and monitoring the ongoing response activities. The team takes the necessary steps to support and facilitate the decision making processes during crisis response, mainly by coordinating the response activities and collecting and distributing information to the responders, senior management, employees and other stakeholders, including the press. The construction of a crisis plan typically starts with an attempt to identify and classify possible crises which may occur, given the properties of the organization and its business processes. Several frameworks have been defined to assist in this classification process (Marcus & Goodman, 1991; Pauchant et al., 1992). Hence, a set of five different incident or crisis types are identified for which a company should prepare (Table 1).

Crisis management entails minimizing the impact of an unexpected event in the life of an organization. Many large organizations have highly developed crisis management plans and teams that are ready and rehearsed for crises. Small businesses, generally defined as those having fewer than 500 employees, may believe that crisis planning is less important. Many small organizations have the mentality that "crises don't happen in our industry/field" or "we have a well-managed business and could manage our way through a crisis without a plan" (Caponigro, 2000). They assume

that crisis events only happen to other organizations or that they are somehow protected from a crisis (Mitroff, 1989). Other small businesses may believe that they need not plan for crises because they carry insurance. Unfortunately, insurance does not cover intangible items such as company reputation, customer goodwill, and professional rapport.

Although terms such as crisis management, crisis plans and teams are well known and different methods are at hand to help companies write a crisis plan, figures on the actual preparedness of companies is rather disappointing. In their 2004 survey, AMA found that 61% of the respondents had a crisis management plan –a slight decrease compared to a year earlier, but still 15% up from 2002. Nevertheless, these surveys point out that no less than 40%of the companies do not have a crisis management plan. These figures are confirmed by the survey of Spillan and Hough (2003) showed that small businesses still place little emphasis on crisis planning. Literature provides us with several possible reasons why so many companies fail to construct a plan: the chance for any serious crisis is perceived too small for it to happen, the conception that insurance covers the damage inflicted by a crisis anyway, or management simply has no idea what the vulnerabilities of their organization are. Regretfully, many excellent case studies now exist describing the fate of organizations that did not have such plans in place (Shrivastava, 1993; Pearson and Mitroff, 1993). They demonstrate that businesses that have no concern regarding a potential crisis will do little to plan for potential occurrences of that event. This, obviously, often results in catastrophic outcomes.

4. Research methodology

The survey consisted of close ended, structured questions, constructed according to the guidelines of Hulshof (1997). It was primarily based upon an earlier national crisis management survey conducted in the Netherlands, Belgium and Luxemburg (Van de Walle et al., 2006), and dealt with four key areas:

(i) experiences and expectations on incidents and crises;

(ii) crisis management activities;

(iii) crisis management plans and

(iv) crisis management teams.

The survey was send to the management of 114 companies in the Turkey. Companies were selected according to the latest data available in the central database of the Chambers of Commerce in the Turkey. The size of the company was a criterion (50 employees or more) as well as the sector to which it pertained (textile and automotive suppliers industries). The survey was anonymous; no identification was required, and results were guaranteed to be treated confidential. A reminder letter was sent to all companies two weeks later. The response rate was respectively 48.2 percent in the textile sectors and 51.8 percent in automotive suppliers (Table 2).

The frequency distribution of the size of the company is expressed in full time equivalents (FTE). It indicates that the majority of responses are from rather small companies, which is no surprise since Turkey is a country with large presence of Small and Medium sized Enterprises (SMEs).

Overwhelmingly, the organizations responding to the survey lacked crisis management teams. Table 3 shows that only 22.8% of respondents acknowledged the existence of a crisis management team, while 71.1% indicated they had no such team. Seven organizations, or 6.1%, did not provide a response to the question. Results of analysis show that, a big majority, small businesses with crisis management teams had no greater concern for potential crises than the businesses without crisis management teams.

Respondents were asked to evaluate the IT implementation level on a five-point scale for three years ago and the research date. Significant increases were registered in the implementation of all individual technologies. As seen in Table 4 IT implementation by Turkish textile and automotive suppliers sectors was low for each IT three years ago. The IT least employed by companies was WAN with a mean score of 3.62 that was followed by MAN (3, 93), LAN (4, 09) and Internet (4, 57). When taking into account current levels of IT, implementation levels increased in a statically significant manner.

Companies were asked whether they recently (i.e., within the last two years) used IT to communicate about their crisis management plans and/or efforts, both within their own organization and towards external parties. They were asked whether they recently used IT to develop or adjust their crisis management plans and whether they used IT for training, simulation or education purposes in the past two years. The results are presented in Table 5.

A vast majority of the companies developed or adjusted their crisis management plans, communicated about crisis management towards their own organization and did some type of simulation, exercise or training in the past two year. Though, crisis management appears to be predominantly an intra-organizational issue. Communication towards third parties is far less common. The use of IT can be observed to be less common. Less than half of the companies that took actions in one form or another use IT to support these actions. Even internal communication regarding crisis management is often not done via IT. This leads to the conclusion that, in general, companies are either not aware of the

ability to support crisis management with IT tools or do not really perceive a high added value of IT for crisis management activities.

5. Conclusions

The work presented in this paper addressed the importance of IT to support the concept of crisis management. This research is based on a large survey in three countries among companies regarding crisis management, resulting in a response of 114 companies. The descriptive analysis of the data points out that the use of IT in crisis management is rather modest. Companies actively involved in crisis management in the past two years used IT in no more than half of their actions taken.

Furthermore, our analysis indicates that crisis management plans primarily impact the perceived need while the presence of a team primarily impacts the level of action taken. Hence, the analysis of risks (first step in the plan) leads to a higher awareness of potential risks and thus a higher perceived need for crisis management, while a team is especially good at introducing actions within a company.

Furthermore, the companies were asked whether or not they had a crisis plan or a crisis team. No enquiry was made into the quality of the plan or team. Hence, in future research, methods need to be developed to incorporate the quality of the latter. Moreover, the response rates were rather low. The survey can be refined by including a distinction for different levels of sophistication of IT use, which can range from the use of mobile phones, PDAs or Personal Computers to the use of dedicated information systems or DERMIS. No clear distinction was made in the current survey.

References

Barton, L. (1993). Crisis in Organizations: Managing and Communicating in the Heat of Chaos. Cincinnati: South-Western Publishing Co.

Booth, SA. (1993). Crisis management strategy—competition and change in modern enterprises. London: Routledge.

Caponigro, J.R. (2000). The Crisis Counselor: A Step-by-Step Guide to Managing a Business Crisis. Chicago: Contemporary Books.

Crandall, W., McCartney, M., & Ziemnowicz, C. (1999) Internal auditors and their perceptions of crisis events. *Internal Auditing*, 14(1), 11–17.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, Vol. 13, 319–339.

Eze, U.C., & Mohammad, N.A. (2000). The influence of information technology on organization structure of Malaysian business firms. *Journal Technology*, Vol. 33(E), 1–10.

Fink, S. (1986). Crisis Management: Planning for the Inevitable. New York: AMACOM.

Hulshof, M. (1997). *Leren interviewen*. Nederlands: Wolters- Noordhoff.

Marcus, A., & Goodman, R. (1991). Victims and shareholders: the dilemmas of presenting corporate policy during a crisis. *Academy of Management Journal*, 34(2), 281-305.

Prebel, J.F. (1997). Integrating the crisis management perspective into the strategic management process, *Journal of Management Studies*, 34(5), 769-791.

Shrivastava, P. (1993) Crisis theory/practice: Towards sustainable development. *Industrial & Environmental Quarterly*, 7(1), 23–42.

Spillan, J.E., & Hough, M. (2003). Crisis planning in small businesses: importance, impetus and indifference. *European Management Journal*, 21(3), 389-407.

Turoff, M., Chumer, M.,Van de Walle, & B.,Yao, X. (2004). The design of a dynamic emergency response management information system. *Journal of Information Technology Theory and Applications*, 5:4, 1-36.

Van de Walle, B., & Rutkowski A.F. (2006). A Fuzzy Decision Support System for IT Service Continuity Threat Assessment. *Decision Support Systems*, 2006.

Van de Walle, B., & Turoff, M. (2006). ISCRAM: Growing a Global R&D Community on Information Systems for Crisis Response and Management. *International Journal of Emergency Management*.

Table 1. Crisis types

Operational Crises	**Publicity Problems**
Loss of records permanently due to fire	Boycott by consumers or the public
Computer systems breakdown	Product sabotage
Loss of records permanently due to computer system breakdown	Negative media coverage
Computer system invaded by hacker	**Legal Crises**
Major industrial accident	Consumer lawsuit
Major product/service malfunction	Employee lawsuit
Death of key executive	Government investigation
Breakdown of a major piece of production/service equipment	Product recall
Fraudulent Activities	**Natural Disasters**
Theft or disappearence of records	Flood
Embezzlement by employee(s)	Tornado
Corruption by management	Snowstorm
Corporate espionage	Hurricane
Theft of company property	Earthquake
Employee violence in the workplace	

Source: Crandall, W., McCartney, M., & Ziemnowicz, C. (1999). Internal auditors and their perceptions of crisis events. *Internal Auditing*, 14(1), 11–17.

Table 2. Response over different industrial sectors

Sector	**Freq.**	**%**
Textile	55	48.2
Automotive Suppliers	59	51.8
Total	**114**	**100.0**

Table 3. Organizations with crisis management teams

Existence of team	**Number of responses**	**Percentage**
Yes	26	22.8
No	81	71.1
Did not respond	7	6.1
Total	**114**	**100.0**

Table 4. Usage of information technologies in companies

Technology items	**3 years ago**		**Current Situation**	
N:114; P<0.010	**Mean**	**St. Dev.**	**Mean**	**St. Dev.**
Internet	4,57	0,66	4,81	0,92
Local Area Network (LAN)	4,09	0,90	4,65	1,03
Metropolitan Area Network (MAN)	3,93	0,86	4,17	0,98
Wide Area Network (WAN)	3,62	1,02	3,91	0,68

Table 5. Use of IT in crisis management

Type of Action	Actions in past 3 years (%)	IT-based actions in past 3 years (%)
External Communication	59	41
Internal Communication	37	25
Crisis Planning	47	59
Plan Development	46	31
Relationship with Media	78	62
Training	63	49
Simulations and Exercises	44	30