JOURNAL OF SMALL BUSINESS STRATEGY

THE DIFFERENCE BETWEEN SURVIVAL AND DISASTER: CRISIS PLANNING IN SMALL BUSINESSES

John E. Spillan
Penn State University – Dubois
jes40@psu.edu

ABSTRACT

Crisis management seeks to lessen the impact of damaging events that can happen to an organization. Although crisis-management literature addressing the needs of larger organizations is plentiful, little has been written on this subject for small businesses. This study examines the perceptions and experiences of crisis events among the owners and managers of small-businesses. The results indicate that few of these organizations have a formal crisis-management team or plan. Reasons for this lack of planning are offered and implications for management are presented.

INTRODUCTION

Crisis management seeks to minimize the impact of damaging events within an organization. Many large organizations have sophisticated crisis-management plans and teams ready to act in the event of a crisis. For small businesses, the opposite is often true. Managers of small operations tend to believe that the issue of crisis management is irrelevant and has limited importance. These organizations might adopt an "it can't happen to us" mentality, assuming that crisis events happen to other organizations or that they are somehow immune (Mitroff, 1989). Other small-business managers believe that they do not need to worry because they have insurance to cover any losses or work interruption. Another reason smaller organizations may not adequately address crisis management is a perceived lack of resources (Barton, 2001). These views are shortsighted and can be detrimental to the success of the small-business operation.

This is a timely topic of special interest to academics and practitioners because we live and work in a turbulent environment. The events of September 11 have changed how many managers do business. Although crisis-management research is expanding, little has been written about crisis-management practices in small businesses. This study provides an overview of crisis-management perceptions of small businesses and empirically investigates three issues:

1. The perceptions of small-business owners and managers regarding the concept and practices of crisis management.

2. Explanations for differences in perceptions and practices that exist in these businesses.
3. Alternatives or recommendations that can strengthen the preparedness of small businesses.

LITERATURE REVIEW

Crisis management

Crisis management aims to limit the impact of an unexpected event. Gorski (1998) reports that a crisis can encompass events from a natural disaster, such as a flood or hurricane, to a form of human tragedy. A crisis can cause an operational production failure and/or it can lead to a public relations fiasco. Subsequent legal problems can disrupt the normal function of business. According to Caponigro (2000), crisis management is the function that helps an organization gain control of the situation. It also poises managers to take advantage of any benefits that a crisis may present, sometimes focusing attention on a business segment that was previously ignored. (Caponigro, 1998; Hickman & Crandall, 1997).

Crisis identification

A. Simbo (1993) reports that one of the major reasons businesses do not have effective crisis-management plans is because they have not identified the potential events that could hurt their organizations. Consequently, they have not developed the tools to deal with a crisis. Fink (2000) contends that crisis identification is important for two major reasons. First, when the crisis is properly defined, it can be managed. Second, once the crisis is defined, it allows managers to determine the influence they have over the desired outcome. Because crises are generally followed by a variety of diversionary problems, it is important that the manager focus interventions on the core issues.

Warwick's (1993) research indicates that one of the important preparations for a crisis-management plan is conducting a risk assessment. Some businesses identify vulnerabilities or crisis events that are unique to their organizations. For instance, movie theaters prepare for the occurrence of a fire with smoke detectors or emergency exits.

The crisis-management literature identifies a number of classifications for crisis events. Some experts have used the cluster analysis (Pearson & Mitroff, 1993). Others have proposed different types of classification methods (Coombs, 1995; Irvine & Miller, 1997). Overall, there is no specific agreement on how to classify crisis events. While the classification systems are important to the researchers, managers need to be more concerned about their unique vulnerabilities (Caponigro, 1998) Thus, this study proposes to ask practicing managers to identify the concerns in their respective organizations. Exhibit 1 summarizes potential crisis categories.

Worst-case scenario planning

Managers must ask: What crisis is of most concern to our business and has such an event or any crisis actually happened? Responses to these questions are important for three reasons. First, as potential crises are identified, managers can begin to plan for them. For example, one of the most difficult crises in a business is the on-site death of an employee. There needs to be a plan to deal with an employee's death in a professional and dignified way (i.e. notifying next of kin). If the worker was instrumental to day-to-day operations, plans must be available to provide a replacement with comparable skill and experience (Wnek, 2000). Second, recognition of potential events enables management to enact measures to prevent them.

Careful planning and the implementation of crisis-management procedures allowed the Y2K transition to occur with minimal difficulties (Salerno, 2000). Finally, identifying the most probable crises allows researchers, writers, and consultants to warn the general business community about crisis events or vulnerabilities that need organizational attention. The Y2K threat was greatly diminished because of the awareness generated by the popular press and management researchers.

Exhibit 1 - Categories of crisis events

Operational crises
- Loss of records permanently due to fire
- Computer system breakdown
- Loss of records permanently due to computer system breakdown
- Computer system invaded by hacker
- Major industrial accident
- Major product/service malfunction
- Death of key executive
- Breakdown of major production/service equipment

Fraudulent activities
- Theft or disappearance of records
- Corruption by management
- Embezzlement by employee(s)
- Corporate espionage
- Theft of company property
- Employee violence in the workplace

Publicity problems
- Boycott by consumers or the public
- Product sabotage
- Negative media coverage

Natural disasters
- Flood
- Tornado
- Snowstorm
- Hurricane
- Earthquake

Legal crises
- Consumer lawsuit
- Employee lawsuit
- Government investigation
- Product recalls

Adapted from: Crandall, McCartney, & Ziemnowicz, (1999). Internal auditors and their perceptions of crisis events. Internal Auditing, 14 (1), 11-1.

SMALL BUSINESSES AND CRISIS MANAGEMENT

Every day small businesses are confronted with unwelcome crises that cause them to crash, strain, struggle and fail in unpublicized silence (Traverso, 2001). Since the terrorist attacks of September 11, many businesses have begun to assess their vulnerabilities. Among small businesses, the task of crisis preparedness has been exceptionally demanding. According to Hopkins (2001), workplace violence, cyber loss and mail contamination are some of the top security issues. One small Houston firm with 110 employees leaves nothing to chance, requiring all job applicants to provide a valid driver's license. Discovery of an invalid driver's license helps managers flag potential problems with an applicant (Hopkins, 2001). Other small businesses are developing systems to back up data to protect against data loss or hacker invasions. Still others are redesigning building space to screen mail for suspicious packages before delivering them to employees (Hopkins, 2001). In 1999, at Hollow Metal Door Co., an employee embezzled nearly $250,000 (Daniels, 2002). While the amount may have been of little consequence to a large company, it was enough to put this small business on the brink of bankruptcy.

A small business's ability to manage a crisis can mean the difference between survival and disaster. Offer's (1998) review of crisis preparedness indicates that 50 percent of all businesses stricken by a crisis will not survive if they do not have an adequate business recovery plan. Pedone (1997) presents an especially pessimistic observation indicating that 90 percent of businesses without a recovery plan would fail within two years of a disaster. Thus, the relevant question in crisis management and planning isn't whether a crisis will occur, but what will it be and when it will occur (Caponigro, 2000).

There is some merit to the argument that insurance will resolve a crisis-provoked problem, but its value is far from complete. Simbo's (1993) analysis of this argument indicates that insurance can provide protection for extensive cost implications, but by itself is inadequate in terms of assuring a firm's survival and recovery. The insurance argument has one major weakness: It does not protect against decreased productivity, loss of goodwill, low employee morale, increased absenteeism, stress, worker unrest, and increased workers' compensation claims (Fink, 2000). The business interruption caused by a crisis can have an impact on customers, suppliers and distributors. Moreover, insurance does not solve the public relations and social responsibility problems that may emanate from the crisis. This point was vividly exemplified in the Exxon Valdez oil disaster (Hartley, 1993). The wildlife and environmental damage could not be valued in dollars and cents. It takes years to recover from such environmental damage; no insurance claim could possibly compensate for it.

Some small businesses argue that they do not adequately develop crisis-management plans because they do not have the resources (Barton, 2001), while others claim that there just is not enough time in today's climate to be preoccupied with crisis-management planning (Caponigro, 2000). While these are understandable points of view, they are imprudent and, if continued, can be harmful to the success of the small business operation. Major deals can be disrupted. It seems more realistic to establish a crisis-management plan to save the company today and then focus on the deals that will come tomorrow

CRISIS PLANNING IN SMALL BUSINESSES: ASSESSING WORST-CASE SCENARIOS

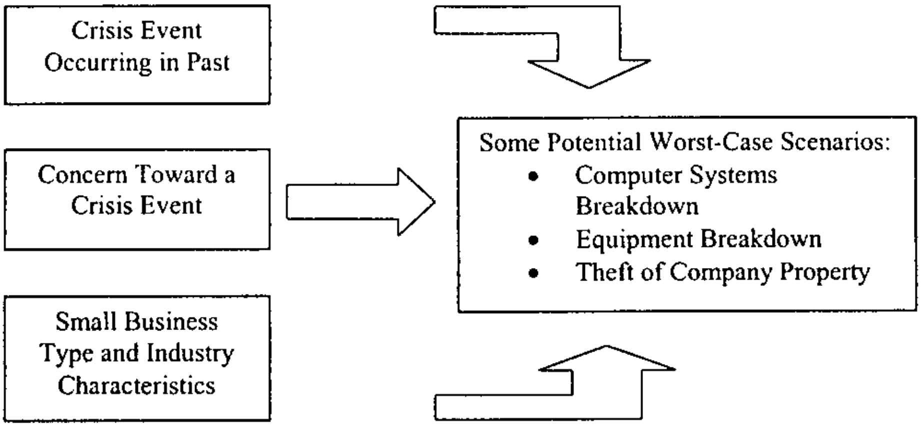
The discussion to this point brings us to the question: What are the crisis events that are of most concern to small businesses? Investigating this question will provide useful insights in determining the worst-case scenarios for the crisis-management process.

Figure 1 presents a format for assessing worst-case scenarios. Three considerations can be evaluated: Has the event occurred in the recent past, what is the current level of concern for that particular crisis, and are there any unique characteristics of the business or industry that would increase the likelihood of a certain type of crisis?

A crisis that has occurred in the recent past is a consideration in worst-case scenario planning. For example, frequent computer system breakdowns can cause major disruptions. Management will want to take steps to prevent their reoccurrence, so *some* planning must take place. A common practice in larger organizations is to have back-up computer facilities in place (hot sites) before a major disruption occurs.

The level of concern about a crisis is important in worst-case scenario planning. While it is expected that concern will increase if a crisis has already occurred, it is also possible that concern may be heightened even if the specific crisis has not occurred. Two examples illustrate this point. First, the Y2K crisis manifested itself at a small number of organizations, although concern for this potential was extremely high. Second, the September 11 terrorist incidents have elevated organizational concerns about similar attacks, even though no attacks have occurred at these organizations.

Figure 1 – Assessing worst-case scenarios



The particular characteristics of a business or an industry and its location may dictate what types of crises should be included in worst-case scenario planning. For example, in Florida hurricanes are included in worst-case scenario planning (Kruse, 1993). The previous discussion on crisis in small businesses has indicated that embezzlement and data back-up are problems that can create a crisis. Businesses would be wise to develop contingency plans for these events.

THE STUDY

Questionnaire

A survey instrument was adapted from the instrument used by Crandall, et al. (1999). The instrument was based on the crisis events listed in Exhibit 1. Respondents were asked to rate their degree of concern for each event, using a scale with 1 indicating a low degree of concern and 5 indicating a high degree of concern. In addition, the survey asked whether the crisis in question had actually occurred at the respondent's organization within the last three years. Respondents were also asked whether their organization had a crisis-management team.

Data collection

The survey instrument was mailed to the human resources or executive offices of 1,000 small businesses in Pennsylvania and New York. Each survey contained a stamped, self-addressed envelope. One hundred and sixty two usable surveys were received – a response rate of 16.2 percent.

RESULTS

Three major business types responded to the survey. These included service business (32.7 percent), manufacturing businesses (35.2 percent), retail businesses (2.5 percent) and a category of "other," which comprised a host of businesses not categorized in any of the above (29.6 percent). Ninety-four organizations (64.4 percent) had fewer than 25 employees, 27 organizations (18.5 percent) had between 25 and 99 employees, 19 organizations (13.0

percent) had between 100 and 499 employees, while 6 organizations (4.1 percent) had over 500 employees. Sixteen organizations did not respond to this question on the survey.

With regard to crisis management teams, seventeen businesses (11.0 percent) said they had a crisis-management team, while 138 organizations (89.0 percent) responded that they did not have one. Seven businesses did not respond to this question.

Data analysis

The first phase of the analysis was to examine the business's perception of crises and crisis management. To determine the degree of concern for a crisis, all 27 items on the questionnaire were measured. The results are displayed in Table 1. The means of each potential crisis revealed a range of scores from 3.76 for computer systems breakdown to 1.22 for an earthquake.

The second phase of the analysis examined the actual occurrences of a crisis event in the last three years. These results also appear in Table 1. The most frequent type of crisis was computer systems breakdown. This crisis occurred at 94 of the organizations, or 59.9 percent of the total number of businesses in the study. The least-frequent occurring crisis was earthquakes, which occurred at three of the organizations.

The next phase analyzed the relationship between the concern for a crisis and the occurrence of a crisis. The purpose of this part of the study was to determine which crisis events happened most often and drew the most concern from the respondents. While it may seem that frequent occurrence of a crisis will generate higher concern, such is not always the case. For example, if computer-system breakdowns have previously occurred in an establishment, but management is not particularly alarmed or concerned about it, then the crisis may not be perceived as severe. When a crisis shows some degree of frequency and a higher degree of concern, then it may be a candidate for worst-case scenario planning. A Pearson correlation analysis found a strong relationship between the concern for a crisis and the occurrence of that same crisis with a coefficient of .734 (significance level $p < 0.01$).

Determining worst case-scenarios

There are various methods to ascertain potential worst-case scenarios. One effective method is to simply ask which crisis events the respondents are most concerned about. These results were revealed in Table 1. Another method is to ask the respondents what events have actually occurred at the organization in a recent time period, such as the last three years, also in Table 1. A third method would be to combine the data from both tables and make a more comprehensive determination of potential worst-case scenarios. For this study, the calculation of Z-scores (Table 2) was used to complete the analysis.

Z-scores were calculated in order to standardize the relationship between these two variables. Using the means scores and the frequency of an event's occurrence presented in Table 1, I calculated a standardized Z-score value. The results of these calculations are presented in Table 2.

Table 1 – Actual occurrence of crisis event & mean degree of concern in last three years

Type of crisis event	Mean Degree of concern	Frequency	%	N=
Computer system breakdown	3.76	94	59.9	157
Snowstorm	2.25	83	56.1	148
Breakdown of a major piece of production/service equipment	3.33	82	53.6	153
Theft of company property	2.67	50	34.7	144
Major product/service malfunction	2.85	45	30.2	149
Permanently lost records due to computer system breakdown	3.26	37	23.7	156
Employee lawsuit	2.70	32	21.9	146
Government investigation	2.52	30	21.1	142
Consumer lawsuit	2.70	26	18.6	140
Flood	1.79	24	16.9	142
Major industrial accident	2.87	23	15.3	150
Product recall	1.96	22	15.3	144
Theft or disappearance of records	2.10	20	13.9	144
Negative media coverage	2.08	15	10.1	148
Embezzlement by employee(s)	1.93	14	9.5	148
Employee violence at the workplace	2.08	13	9.2	142
Product sabotage	1.73	10	6.6	151
Death of a key executive	2.60	10	6.9	145
Hurricane	1.35	9	6.2	146
Computer system invaded by hacker	2.24	9	5.9	153
Corporate espionage	1.71	7	4.9	144
Tornado	1.51	6	4.2	142
Lost records permanently due to fire	2.25	5	3.2	155
Corruption by management	1.71	4	2.7	147
Boycott by consumers or public	1.52	3	2.0	153
Earthquake	1.22	3	2.0	147

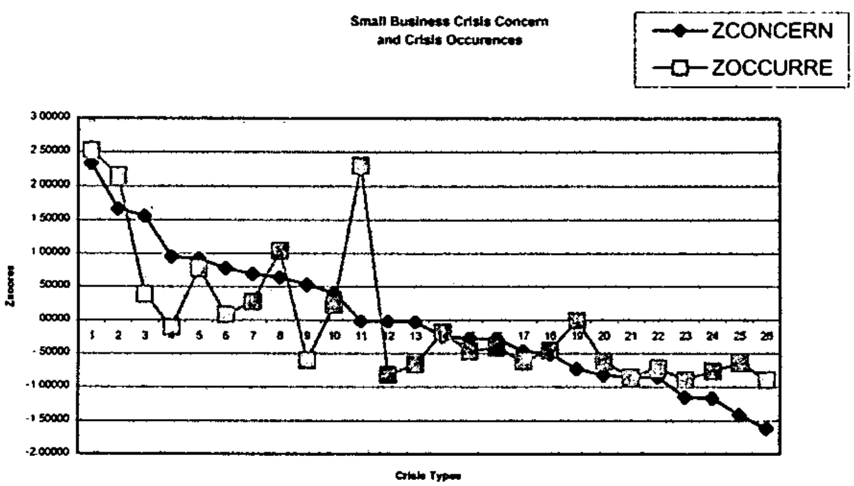
Z-scores standardize the variables according to the number of standard deviations from the mean of the sample. The higher the Z-score, the farther away from the mean is the variable. Z-scores of 0 equal the mean for the sample; therefore scores over 0 were of particular interest in this study because they indicated higher degrees of concern or occurrence than the sample's average. To help visually depict this relationship, an examination of Graph 1 reveals nine potential crisis events where both Z-scores for concern *and* occurrence are over 0. Using the Z-score greater than 0 criterions, I propose that these events are good candidates for worst-case scenario planning. Graph 1 illustrates how occurrence and concern move together for each crisis. Not every event follows this pattern on a smooth curve. For example, major industrial accident (item 4,) and consumer lawsuit (item 6, among others) deviate to a greater extent from the concern curve.

Table 2 – Z-scores for degree of concern and occurrence of an actual crisis

	Number key to type of crisis event	Z-score for degree of concern for the crisis	Z- score for occurrence of crisis
1	Computer systems breakdown	2.333451	2.52353
2	Breakdown of a major piece of prod/serv. equip	1.66546	2.115164
3	Permanent lost records due to computer breakdown	1.55654	.38665
4	Major industrial accident	.94972	-.10921
5	Major product/service malfunction	.91860	.77034
6	Consumer lawsuit	.77857	.08559
7	Employee lawsuit	.68521	.28039
8	Theft of company property	.63853	1.03598
9	Death of a key executive	.52962	-.60506
10	Government investigation	.40514	.23317
11	Snowstorm	-.01496	2.29922
12	Lost records permanently due to fire	-.01496	-.82347
13	Computer invaded by hacker	-.03052	-.66409
14	Theft or disappearance of records	-.24835	-.19185
15	Employee violence in the workplace	-.27947	-.46929
16	Negative media coverage	-.27947	-.41616
17	Product recall	-.46618	-.62277
18	Embezzlement by employee(s)	-.51286	-.45158
19	Flood	-.73069	-.01476
20	Product sabotage	-.82405	-.62277
21	Corruption by management	-.85517	-.85298
22	Corporate espionage	-.85517	-.72312
23	Boycott by consumer or public	-1.15080	-.89430
24	Tornado	-1.16636	-.76444
25	Hurricane	-1.41531	-.64638
26	Earthquake	-.61758	-.89430

Graph 1 - Z scores for degree of concern and occurrence of actual crisis

Pearson correlation = .734 (p<. 01)



DISCUSSION

Analysis of the data reveals two major themes: first, the major crises that small businesses need to address; second, the findings suggest that few small businesses have established crisis-management teams or plans for dealing with a crisis.

What are the worst-case scenarios?

Discovering the worst-case scenarios that will determine the content of crisis plans is part art and part science. In the final analysis, the specific worst-case scenarios will be a function of the individual organization within the context of its size and industry. This study analyzed the scenarios from an aggregate point of view, i.e., the sample was not further subdivided into segments such as industry or organization size. The events that meet this criterion include:

- Computer systems breakdown (Zconcern = 2.333, Zoccur = 2.523)
- Breakdown of a major piece of prod/service equipment (Zconcern = 1.665, Zoccur = 2.115)
- Permanently lost records due to computer breakdown (Zconcern = 1.556, Zoccur =0.3866)
- Major industrial accident (Zconcern = 0.9497, Zoccur = -0.1092)
- Major product/service malfunction (Zconcern = 0.9186, Zoccur = 0.7703)
- Consumer lawsuits (Zconcern = 0.7785, Zoccur = 0.0855)
- Employee(s) lawsuit (Zconcern = 0.6852, Zoccur = 0.2803)
- Theft of company property (Zconcern = 0.6385, Zoccur = 1.0359)
- Death of a key executive (Zconcern = 0.5296, Zoccur = -0.6050)
- Government investigation (Zconcern = 0.4051, Zoccur = 0.2331)
- Snowstorm (Zconcern = -0.0149, Zoccur = 2.2992).

These findings show that 5 of the 11 potential crisis events involve significant business operations. Even though they may seem to be challenging, these potential events could be controlled to some degree by the organization itself. Computer systems data and equipment can be backed up. Expanded or more focused quality-control measures can be implemented to assure that product/service malfunctions and industrial accidents are mitigated. These management practices need periodic assessment to ensure that they are effectively and continuously applied in the work environment.

IMPLICATIONS FOR MANAGEMENT

This finding reveals an important challenge in crisis planning. If a business has not experienced a crisis or no vulnerability is identified, then planning for it is not considered a priority. Management books and the popular press continuously report and discuss case studies of businesses of all sizes that failed because they were unable to manage a crisis event. The challenge then, is to convince all owner/managers, particularly those of small businesses, of the need for proper crisis management.

Table 1 indicates that there is genuine concern about potential crisis events such as breakdown of a major piece of production/service equipment, major industrial accident, computer-system breakdown, and flood just to mention a few.

Managers and small-business owners need to think seriously about taking steps to avoid a crisis. Focusing on the following ideas will go a long way toward that end:

1. Form a crisis-management team.
2. Know how to detect crisis symptoms or conduct vulnerability analysis.

3. Develop an effective communication mechanism within the business.
4. Train everyone to be vigilant, prepared and responsive.
5. Remain flexible to changing environments.

The first recommendation is for a small business to form a crisis-management team. No matter how small the business, an appropriate team can be established. It may be only the owner and one staff person, but that is sufficient. In a larger business, the team should consist of key company representatives from operations, marketing and accounting, as well as the CEO or owner. If the team is new, it is may be worthwhile to consult with experts who can provide a framework for operation. (Fink, 2000). While the size of the team depends on the particular type of business, it is suggested that it be kept to fewer than 10 members (Barton, 1993).

The second recommendation focuses on a vulnerability analysis. One of the most important steps in developing the crisis-management plan is to identify most significant vulnerabilities in the business and prioritize them. The best way to do a vulnerability analysis is to ask questions and be perceptive about warning signs (Caponigro, 2000). A business that plans for a crisis unique to its industry becomes better prepared to manage the crisis should it occur.

The third recommendation centers on making the communication system as effective as possible. Communicating during and after a crisis is crucial to successful crisis management. One essential element of this process is the selection of a proper spokesperson. To achieve competency in this area, it may be necessary to seek the expertise of professionals in communication techniques (Caponigro, 2000).

The fourth recommendation suggests ongoing training of personnel. Offering both formal and informal training to management and employees is an important ingredient in the crisis-management equation. The more knowledge an employee has about the warning signs of a potential crisis, the easier it is to identify the crisis and deal with it immediately. This is why creating a corporate culture that is sensitive to the crisis-management concept is so important.

Finally, it is recommended that the crisis-management team and business personnel remain flexible. In managing a crisis, the decision-makers must not be locked into inflexible plans. Responding to a crisis is a fluid process (Fink, 2000).

CONCLUSION

This study investigated the perceptions and experiences of small businesses as they relate to worst-case scenarios. The results indicate that, in general, small businesses are not that concerned about crisis issues and subsequently, few have crisis-management teams. One reason this may be the case is that smaller businesses experience fewer crisis events relative to larger organizations. Another reason could be that because a majority of the businesses have fewer than 25 employees, they do not believe that they have the resources for a crisis-management process.

There lies the paradox. Because of those fewer resources and lack of expertise, small businesses are also less likely to recover if they do experience a crisis. This study concludes that small businesses, like their larger counterparts, should adopt crisis-management plans. They should incorporate worst-case scenario identification and crisis planning in their business-development plan. Reading *The Small Business Owner's Guide to A Good Night's Sleep*, by Debra K. Traverso, provides practical strategies for identifying worst-case scenarios and managing them.

Study's contribution to crisis management

While the study is exploratory, it does contribute to the understanding of crisis management. First, it provides insight into the types of crises and crisis concerns that small business managers consider important to their operations. These insights form the basis for worst-case scenario planning.

A second contribution addresses the association between concern for a crisis and its actual occurrence. The study reveals that concern and frequency move in the same general direction, i.e., high-concern events have also occurred more frequently while low-concern events have occurred less frequently. One obvious caveat should be noted. The terrorism of September 11 was, statistically, a rare event. And yet, concern for terrorism has increased dramatically in the United States, even though the incidence of terrorism is low. In crisis management, it is understood that some events have a low likelihood of occurring, yet they still generate high concern among managers.

REFERENCES

Barton, L. (1993). *Crisis in organizations: Managing and communicating in the heat of chaos*. Cincinnati, OH: South-Western Publishing Co.

Barton, L. (2001). *Crisis in organizations II.* United States: South-Western Publishing Co.

Caponigro, J. (1998). The crisis counselor. *The executive's guide to avoiding, managing, and thriving on crises that occur in all businesses.* Southfield, Mich.: Barker Business Books, Inc.

Caponigro, J. R., (2000). *The crisis counselor: A step-by-step guide to managing a business crisis.* Chicago: Contemporary Books.

Coombs, W. (1995). Crisis response strategies. An exploratory study. *Proceedings of the 3rd Annual Conference on Crisis Management, Las Vegas: Nevada.*

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

Daniels, C. (2002, May). Confessions of an embezzler: *FBS- Fortune Small Business*, http://www.Fortune.com/fortune/print/0,15935,361268,00.html, pp. 1-5.

AMACOM. (2000). *Crisis management planning for the inevitable.* New York: Fink, S.

Gorski, T. (1998). A blueprint for crisis management. *Association Management, 50* (1), 78-79.

Hartley, R. (1993). *Business ethics: Violations of the public trust.* New York: John Wiley & Sons.

Hickman, J., & Crandall, W. (1997). Before disaster hits: A multifaceted approach to crisis management. *Business Horizons, 40* (2), 75-79.

Hopkins, J. (2001). Small businesses take steps to protect themselves. *USA Today*, 20(43), 6b

Irvine, R., & Millar, D. (1997). Multiplying the effects. Factors influencing media coverage of business crisis. *Proceedings of the 6th Annual Conference on Crisis Management, Las Vegas: Nevada.*

Kruse, C. (1993). Disaster plan stands the test of hurricane. *Personnel Journal, 72* (6), 36-43.

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.

McCartney, M., Crandall, W., Ziemnowicz, C. (1999). Why plan for something bad if it may not happen? Or is all this crisis management stuff just another fad?. *Internal Auditing, 14 (1)*, 11-17.

Megginson, W.L., Byrd, M.J. & Megginson, L.C. (2000). *Small Business Management. An Entrepreneur's Guidebook.* Boston: Irwin-McGraw-Hill

Mitroff, I.I., (1989). Programming for crisis control. *Security Management,* October, 75-79.

Offer, J. (1998). Pessimist's charter. *Accountancy, 121* (4), 50-51.

Pearson, C., & Mitroff, I. (1993). From crisis prone to crisis prepared. A framework for crisis management. *Academy of Management Executive, 71*, 48-59.

Pedone, R. (1997, November 3). Disaster recovery , are you prepared for business disruption? *Long Island Business News*, Nov. 3, 23-24.

Salerno, C. (2000). Walking on sunshine. *Contingency Planning & Management*, 5 (3), 10-14.

Simbo, A.K. (1993). Catastrophe planning and crisis management. *Risk Management, 40* (2), 64-66.

Traverso, D.K. (2001). *The small business owner's guide to a good night's sleep.* Princeton: Bloomberg Press.

Warwick, M. (1993). Disaster recovery: Come hell or high water. *Communication International, 20* (10), 33-40.

Wnek, R. (2000). Helping employees recover. *Contingency Planning & Management*, 5 (4), 26-29.

***John E. Spillan**, M.B.A. and Ph.D. in Business and Management and serves as Assistant Professor of Business Administration at The Pennsylvania State University –DuBois Campus. His research interests center on Crisis Management, Marketing and Entrepreneurship and International Business with specific interest in Latin America and Eastern Europe. His articles have appeared in the Journal of Business, Management Development Forum, International Journal of Marketing and Marketing Research, Journal of Business in Developing Nations, Southern Business Review and Communication Research Report. Dr. Spillan is coordinator of the Bachelors of Science in Business degree program at the Penn State-DuBois campus. He has traveled extensively in Europe, Latin America and the Middle East.*