Modifications in Risk Management in the Financial Sector in the Post 9/11 World; A Situational Analysis

Kaushik Ghosh

Department of Management Information Systems & Decision Science
Texas A&M International University
5201 University Boulevard
Laredo, TX 78041-1900
email: kaushik7778@rediffmail.com

Stephen E. Lunce

Business Computer Information Systems Department
College of Business Administration
Midwestern State Univerity
3410 Taft Blvd.
Wichita Falls, TX 76308
(940) 397-4046
email: stephen.lunce@mwsu.edu

Balasundram Maniam

Sam Houston State University
Department of General Business & Finance
P.O. Box 2056
Huntsville, TX 77341
email: maniam@shsu.edu

ABSTRACT

This paper provides a situational analysis of the impact that the attacks of 11 September 2001 had on the financial sector of the economy. The paper will provide some general comparisons of disaster recovery or business continuity planning in the financial sector in both the pre-9/11 and post-9/11 economies. It will then present specific changes that have occurred in the planning activities of several major firms, including Citigroup and Bank of America. Finally, it will suggest some general implications for management – specifically business continuity planning – in the wake of the attacks of 11 September.

INTRODUCTION

Prior to the 11th of September 2001, many studies had suggested that wide sectors of American business were not well prepared for disasters. While many firms had developed or considered developing disaster recovery (D.R.) or business continuity (B.C.) plans, the extant plans often only existed on paper, and the majority was rarely – if ever – tested. The 9/11 attacks on New York's World Trade center illustrated how woefully unprepared many firms actually were. In the wake of the 9/11 attack, it would seem reasonable to assume that almost all firms would improve their disaster recovery plans. Unfortunately, this has not been the case. "In places such as

Omaha, Peoria, and Kansas City [executives] respond with 'our country's preparedness has increased and targets are likely to continue to be large metropolitan cities…The probability is very low that it won't happen … and [we] are will to take the risk" (Walch, 2004, p. 72).

When ill-equipped organizations are hit by disasters, the consequences can be varied and diverse. Organizations can not only suffer from financial instability, but their reputation can be tarnished. In today's business environment, which is demanding as well as unforgiving, organizations seeking to maximize profits must minimize risks. "Risk management is a systematic process of analyzing every possible unfavorable and undesirable outcome [of a potentially destructive situation] and developing strategies to avoid, minimize or cope with the impact" (adapted from the Washington State Department of Information Services, http://www.dis.wa.gov/pmframework/planning/riskmgmt.htm).

The financial sector of industry in the United States is one of the most regulated components in the economy. It would seem that following the attacks of 9/11, where shortcomings were identified, and where plans did not allow organizations to recover or continue, these newly identified limits in the ability of firms to continue would lead to radical changes in D.R. plans. In studies following the attacks, 48 percent of managers said that they had become more aware of threats to their information, and 47 percent said their firm was planning to send more on security, including disaster recovery in the future (Turban, 2004). This paper reviews how some selected firms in this sector have changed their approaches to B.C. and D.R. planning in the wake of these attacks.

DISCUSSION

Risk Management Planning

According to the State of Washington's Information Services group, risk management comprises two basic activities: risk assessment and risk control/reduction (Washington State Department of Information Services, www.dis.wa.gov/pmframework/planning/riskmgmt.htm). Risk assessment follows the basic risk paradigm as defined by MacCrimmon and Wehrung (1986); this paradigm will be described briefly in the next paragraph. However, this paper focuses on the risk control aspect of risk management; this discussion will present the cases of several well-known financial entities (e.g. Morgan Stanley, Citigroup, and Bank of America) and analyzes how they have modified their B.C. procedures in the wake of the 9/11 attacks.

The basic risk paradigm can be envisioned as a three outcome decision tree (Lunce, 1994). "Risk is generally considered to be the antithesis of benefit. It is … diametrically opposed to profit or gain; it cancels out opportunity; it offsets the chance of succeeding. Thus it is negative and undesirable factor with which managers must reckon" (Grose, 1987, p. 24). The decision maker considers this negative outcome and must select must select from one of the three outcomes. The initial choice is between a sure action, wherein the decision maker knows the results of the choice, in advance; the alternative is a risky decision. This risky decision also presents a dual alternative, one of which provides a better resultant situation than the other. The better solution provides a chance of gain or profit, and the lesser is described as a chance of loss or loss income (MacCrimmon and Wehrung, 1990).

Controlling Risk

A contingency plan forms the basis of risk control/reduction and disaster recovery plan is essentially a part of the total contingency plan to minimize loss of life and property in response to physical threat (Nursey, 2003). Several models of contingency plans have appeared in the literature; all have helped illustrate how to deal with the challenge of managing risk. One of most elegant is the model used by the European Space Agency (ESA). It is illustrated in the following figure.

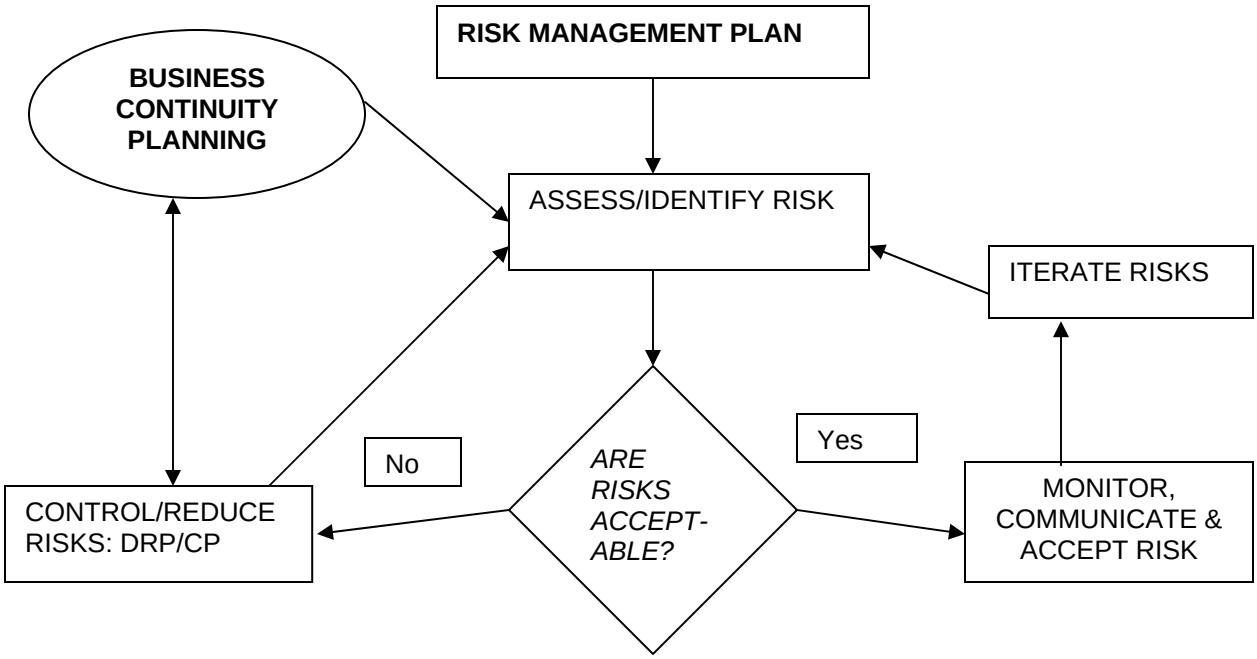

Figure 1: Role of Disaster Recovery/Contingency Plan in Risk Management Plan
(source: European Space Agency, www.estec.esa.nl/pr/qq/risk/introduction/q2.htm)

The above figure clearly depicts that when risks are not acceptable, risk control measures need to be deployed. In other words disaster recovery plan needs to be present as a risk control initiative. Disasters are either natural (earthquakes, tornadoes, cyclones etc.) or man-made. In the recent years companies in the United States have encountered several man made and natural disasters. Studies have suggested that terrorism, as a form of man made disaster has become a source of major threat to the business world. Acts of terrorist attacks on American soil are almost certain to occur in the future. Though terrorist's attacks don't eventually succeed in accomplishing their primary objective which is generally to destabilize a government, the magnitude of disaster can be immense to the affected target. The terrorist's primary motive is destruction or undermining the government's credibility for some purpose or reason. In the western world political change is brought about by the people or the governed. In order to destabilize and tarnish the image of the government so that the governed loose faith in the government's abilities and eventually have it replaced, the terrorists engage in heinous acts. Usually they are not successful in bringing about the political change that is their aspiration.

However, terrorist threats are part of today's reality, and they are a potent source of risk. In their attempt to destabilize the capitalistic economy of the United States, terrorist targeted the symbol of success of America – the corporate world. The World Trade Center was home to some of the leading companies of the world, and its targeting illustrates the intentions of Al-Qaeda. Business managers who are responsible for contingency planning need to consider the terrorism threat along with the threats posed by the natural disasters like cyclones, tornadoes, earthquakes. The magnitude and ferocity of the terrorist attacks of 11 September reveal one harsh reality – that organizations must be prepared for the worst possible disaster (Sjoberg, 2004).

Risk scholars argue that the scale of the 9/11 disaster could have been similar to that caused if a major natural disaster (e.g. tornado/cyclone/earthquake) hit the World Trade Center. Analysis of the post 9/11 B.C. strategies indicate that, with few exception such as Merrill Lynch, most firms are still not prepared to counter the non-natural risk of terrorist attacks. But whatever was the ultimate outcome, post 9/11 investigations of business resumption strategies revealed that companies with an exception of a few (e.g. Merrill Lynch) were not equipped to counter disasters due to terrorism (Lunce, 1994).

General Changes in Risk Management after 9/11

Prior to 9/11

- Disaster recovery planning comprised of basic procedures like making back up copies of data. Disaster recovery procedures were only important to a certain extent, and always subject to cut backs during lean periods (Tanner, 2004).
- Organizations consigned business continuity and disaster recovery strategies to middle and lower level management, hence clearly undermining the importance of D.R. planning (Pallatto, 2002).
- Market analyst, *Meta Research*, says 50% of the global 2000 companies had credible Disaster recovery plans (Adshead, 2003).

Post 9/11

- Senior management of organizations has begun to take serious interest in creating a business continuity plan and having in place the best possible disaster recovery plan to minimize and control losses in the worst possible scenario (Adshead, 2003).
- The scope of disaster recovery planning/contingency planning expanded beyond computer room doors. The people responsible for the business functions of a company are becoming more involved, besides those who are associated with formulating technological changes in the company (Rothstein, 2002)**.**
- General awareness has increased, but executives in many areas have been slower to react than might have been expected (Walch, 2004).

EXAMPLES FROM THE FINANCIAL SECTOR

This section of the paper will discuss briefly how several selected organizations changed their approaches to risk management in the wake of the September 11th attacks on the World Trade Center. The firms that will be considered are: Morgan Stanley, Bank of America, Bell Telephone, and Citigroup. The discussion of each will be in two parts: a pre-9/11 status and changes implemented as a result of the attacks on the World Trade Center. All data discussed are available in the public domain; no confidential information will be revealed.

General Financial Sector Comments

Several governmental rules have been in place to insure that electronic data and financial information is protected. For example, the Internal Revenue Service (IRS) Procedures 64-12 and 71-20 require that firms must be able to reconstruct recorded data and such data must be auditable – even after a disaster – in accordance with the Internal Revenue Code of 1954 (Toigo, 1989). National banks and financial institutions insured by the Federal Deposit Insurance Corporation (FDIC) must also comply with the 1983 Banking Circular 177 (BC-177) which "makes bank management responsible for determining critical functions at the bank, assessing the risk and potential impact of loss" of electronic data (Toigo, 1989, p. 10). However, in spite of the many federal regulations, the financial industry had not done enough to prepare for the devastation that might occur from a terrorist attack (Swann, 2004).

Disaster recovery and business resumption plans have become mandatory for all federally supervised financial institutions. The financial industry has become more aggressive in the implementation of comprehensive D.R. plans than other industry sectors (Tanner, 2004). This industry has become the leader in the private sector with regards to investments and expenditure on B.C. plans. The industry's spending has had a 26% increase from 2001, and an increased interdependence amongst the financial system participants, irrespective of the geographic location has been developed (Swann, 2004).

Other specific recommendations and suggestions were presented on 9 May 2002 by Roger Ferguson, Jr., Vice-Chairman of the Federal Reserve. These ideas were included in a presentation to the Federal Reserve Board.

- Business resumption plans need to be expanded to provide for wide-scale and regional events (Ferguson, 2002).
- Business resumption plans should also take into account the loss or inaccessibility of staff (Ferguson, 2002).
- Vulnerabilities are associated with the current geographic concentration of financial market participants and some of their backup facilities. Hence geographic diversity for critical operations and backup facilities should be a key consideration of business-resumption plans (Ferguson, 2002).
- Business continuity arrangements should be effective and compatible within and across institutions. The industry can accomplish this effectiveness and compatibility only through developing multiple levels of backup, depending on the criticality of the function or business line (Ferguson, 2002).

- Financial industry participants must engage in vigorous testing of their contingency plans and backup facilities (Ferguson, 2002).
- Business-resumption plans should reflect recovery-time. Previous assumptions about how long backup facilities may need to be used and their capacity levels should be revised to incorporate the possibility of longer-term disruptions and to accommodate normal or increased volume of transactions (Ferguson, 2002).
- Financial institutions should look for alternatives to telecommunications services, like Internet, satellite, and wireless services (Ferguson, 2002).

Morgan Stanley

Prior to the 9/11 attacks, back up office space was close to the company's headquarters; its trading and back-up facilities were concentrated in two buildings within the same block. Consequently, both of the company's buildings (main headquarters and the back-up site) were dependent on the same transportation grid and power infrastructure; an attack as destructive as 9/11 could have damaged or destroyed both headquarters and back-up buildings leaving the firm in an almost impossible situation to be able to maintain operations (Vidal, 2002). The company decided to move to a more dispersed environment-for workers, executives, IS and its communication systems. The company also sold its newly acquired back-up space site (since it was close to its headquarters) and moved their business operations in downtown Manhattan completely out of New York City (Schmelkin, 2002).

Bank of America

Following the Loma Prieta earthquake of 1989, Bank of America executives were relatively pleased with the firm's response to this natural disaster. The quake occurred at 17:04 PST, and the following day the bank's customers saw little disruption in service except for the inability to use ATMs in the Bay Area. The interruption of ATM service was a result of a total loss of electrical service, rather than damage to the system. While customers saw no interruptions, Directors Longworth and VanderVliet (1991) report, "Internally, it wasn't exactly business as usual but we carried out critical functions…all posting systems operated in a normal manner" (p. 247). Unfortunately, the firm discovered after the event that many decisions were made based solely upon information that was provided by television news.

They have gone on to change their disaster recovery plan based on the changing projections about the size, nature and probability of attacks. It has put emphasis on developing response teams and it has also started to conduct quarterly tests to check for the efficiency of their plan (Julavits, 2003).

SBC Telephone

Since the divestiture in 1984, disaster recovery has been a part of the corporate culture at SBC. However, the focus had been on natural disasters (hurricanes, tornadoes, and floods), any of which could negatively impact a communications company's ability to provide service to its subscribers (Bischoff, 2004).

Observing the struggles endured by Verizon as it tried to restore service in Lower Manhattan following the 9/11 attacks, SBC executives determined that their D.R. plans needed to be modified. In the wake of the attacks, it has developed a more comprehensive plan which takes into consideration manmade calamities (Bischoff, 2004).

Citigroup

Prior to the attacks of September 11, B.C. planning was handled in various local and regional facilities. Robert Druskin, Citi's Chief Operations and Technology Officer described the expense and difficulty of exercising B.C. plans, and how those difficulties had inhibited Citi's development of more comprehensive plans (Costanzo, 2002).

In the aftermath of the attacks Citigroup established several new initiatives. It set up a bioterrorism group to develop procedures for handling suspect mail; this group was composed of personnel with governmental and medical backgrounds. Perhaps the most important step taken by Citigroup was the appointment of a head of business continuity, who would lead "a new committee to ensure business-continuity best practicesget shared across the company..." (Costanzo, p. 2). Prior to this appointment, there was no one "at the Citigroup level responsible for business continuity" according to Druskin (Constanzo, 2002, p.3).

SITUATION ANALYSIS

Immediately following the 9/11 attacks D.R. planning and B.C. planning were high priorities in most, if not all, sectors of the economy including the financial sector. However, economic constraints have lead to a declining level of enthusiasm for investment in planning for events that have only a small probably of occurrence (D'Antoni, 2003).

A study of 300 business technology executives, conducted by *Informationweek*, found that interest in, and budgetary commitments for B.C. planning were declining in the wake of the 9/11 attacks. In 2002, seventy-seven percent (77%) of respondents indicated that their firms were budgeting for disaster preparedness in some form. In 2003, only sixty-five percent (65%) of the same group responded that their firms were continuing to budget for disaster recovery planning. The decline was blamed on the weakness of the economy (D'Antoni, 2003).

The decline in interest as represented by a decline in budget is more evident in smaller firms. Figure 2, from *InformationWeek Research* illustrates this decline.

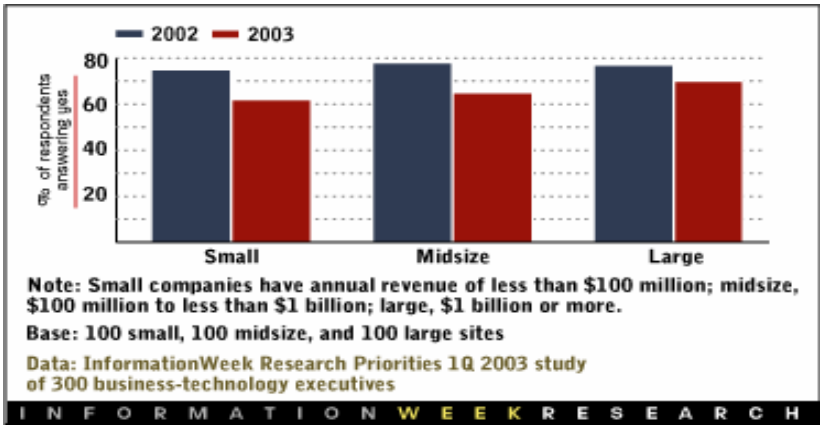

Figure 2: Disaster Recovery Planning Budgets – 2002 versus 2003

As the figure above shows, DRP/CP has less importance among all companies in 2003 than in 2002. The change is much greater in small and midsized firms than in large companies, but the decline in commitment of resources in 2003 is evident among all respondents (D'Antoni, 2003, p. 63).

Organizations need to balance between the business risk they could withstand and the costs associated with implementing recovery plans in the event of a disaster. Ideally, all companies would not want to lose any data and have zero downtime. But planning and protecting to achieve zero loss of data and no downtime is a too good to be true and very expensive proposition. All systems and business processes cannot be termed equally mission-critical. Hence companies need to have recovery time objectives (RTO) to provide them with guidelines when disruptions occur. RTO help in determining the time required to recover mission critical operations, consequently minimizing downtime. Recovery point objectives (RPO) help in minimizing data loss. "Business continuity plans start by determining the RTO and RPO for a particular company's applications. The relative importance of RTO and RPO is different for every organization. For example, an e-commerce Web site may tolerate a higher RPO than RTO, because while the business cannot afford to be off-line, orders that end up backlogged may not affect the customer experience as negatively. A financial services firm, however, would likely have close to zero RTO and RPO because not only does it need to be up and running quickly, but also the large majority of financial services firms store most of their files electronically. Brokers, for example, need immediate access to their up-to-date files so the business can move forward serving and handling transactions on behalf of its clients" (Cramer, 2004, p.2).

SUMMARY

According to the Milken Institute report, there are major economic losses that have affected both the national and metropolitan economies since September 11. Several Industries have been affected including travel and tourism, airlines, entertainment, financial services, and retail. Defense and aerospace have been positively impacted by future spending in this sector. The economic impact of the attacks can't really be compared to a natural disaster as it has had more

far reaching geographical effects that will last much longer than a natural disaster. The technology sector was one of the main reasons for the slow economy prior to the attacks. Manufacturers, retailers, and exporters will recover, however it will be at a conservative pace. An underlying factor to the recovery of the economy will be continued stability and the prevention of future catastrophic events, especially terrorism (Devol, 2002).

Prior to the terrorist attacks of 11 September 2001, many firms, many sectors of the economy, and many governmental agencies had developed disaster recovery or business continuity plans. Most managers of these organizations were confident that the firm would survive any natural or man-made disaster, and the literature is replete with examples of first that survived the seemingly overwhelming catastrophe. The cost of the attacks was measured in billions of dollars, thousands of lives, and tens of thousands in lost jobs. Estimates suggest that more than 50% of the three hundred firms located in the World Trade Center were not able to remain in operation. The financial sector suffered severely; the New York Stock Exchange closed for six days following the attack. Three years later the U.S. economy still has not fully recovered, and the travel industry – with increased security restrictions – may never return to its glory days.

The attacks demonstrated several needs. Firms can no longer rationally assume that structures will survive a disaster, nor can they assume that municipal infrastructures will survive. Almost 3,000 people died in the twin towers; many of them were executives, managers, decision-makers whose responsibilities had to be carried out by others, if they were carried out at all. Information that was assumed to be safe, and the processes needed to produce that information, was destroyed. The communications networks that decision-makers relied upon were gone. The ability to move to alternate processing sites was inhibited. Business continuity plans have to become more comprehensive and inclusive.

In general, the United States was heavily impacted by the terrorist attacks on the World Trade Center Towers and the Pentagon on September 11, 2001. There was a notable chain reaction that occurred when the U.S. financial markets were impacted which began with a significant drop in trading that resulted in a loss in consumer confidence. As consumers' confidence diminished, they stopped spending and started saving their cash. The reduction of cash flow reduced companies' profits and revenues, thereby leading to downsizing. By reducing jobs it raised unemployment and ultimately has led to a recession. On a national level, legislators have reacted to the terror in swift, calculating ways in order to stabilize the economy and reassure Americans that safety is and will be paramount. Although, as the economy slowly started its road to recovery, the possible risk for future attacks is always in many average Americans' mind, let alone investors, but they all take one day at a time (Devol, 2002).

REFERENCES

Adshead, A., (2003). "The Future of the IT Organization," *ComputerWeekly.com*, 9 September 2003, [on-line] viewed at www.computerweekly.com 13 September 2004.

Bischoff, G., (2003). "Masters of Disaster," *Telephony*, 18 August 2003, [on-line] reviewed at http://telephonyonline.com/ar/telecom_masters_disasters/index.htm, 13 September 2004.

Costanzo, C., (2002). "Citi Upgrades Disaster, Terror Plans," *American Banker,* 167 (49), 13 March 2002, pp. 2-3.

Cramer, B., (2004). "Business Continuity Metrics: How Much Can You Afford to Lose?" *ComputerWorld,* 4 May, [on-line] reviewed on 11 September 2004 at http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,92865,00.html

D'Antoni, H., (2003). "Business Continuity Slides Down the Priority Scale," *Informationweek,* Issue 992, p. 61-63, 13 January.

Devol, R. C., et al (2002). "The Impact of September 11 on U.S. Metropolitan Economies." *Milken Institute*, Santa Monica, California, January.

Ferguson, R.W., Jr. (2002). "Implications of 9/11 for the Financial Services Sector," remarks to the Conference on Bank Structures and Competition, Chicago, IL, 9 May.

Grose, V.L., (1987). *Managing Risk, Systemic Loss Prevention for Executives*, Prentice Hall, Englewood Cliffs, N.J.

Julavits, R., (2003). "Evolving Disaster Planning at B. of A.," *American Banker,* 168 (30), 13 February 2003.

Longworth, T.R. and VanderVliet, R., (1991). "Contingency Planning at Bank of America: the Loma Prieta Experience," *Disaster Recovery World,* Disaster Recovery Journal, St. Louis, MO, p.247.

Lunce, S., (1994). "An Examination of the Managerial Issues Involved in the Contingency Planning for Information Systems," University of Texas at Arlington.

MacCrimmon, K.R. and Wehrun, D.A., (1990). "Characteristics of Risk Taking Executives," *Management Science,* 36 (4), April, pp. 422-435.

Nursey, H.V., "Information Security in General Medical Practice," [on-line] reviewed 11 September 2004, www.nevdgp.org.au/isgemp/Homepage.htm, 22 October 2003.

Pallatto, J. (2002). "Interview with Gary Hilbert," *Internet World Magazine*, [on-line] reviewed 11 September 2004, www.internetworld.com, 1 May 2002.

Rothstein, P.J. (2002). "September 11 Changes Everything," Rothstein Associates, Inc., [on-line] viewed 6 September 2004.

Schmelkin, A. (2002). "Disaster Anticipation Has Two on Move," *American Banker,* 167 (19), 29 January.

Sjoberg, L. (2004). "The Perceived Risk of Terrorism," SSE/EFI Working Paper series in Business Administration No. 2002:11, Center for Risk Research, Stockholm School of Economics, Stockholm, Sweden, 16 January 2004, available on-line at: swoba.hhs.se/hastba/papers/hastba2002_011.pdf, reviewed 12 September 2004.

Swann, J. (2004). *Community Banker,* 13 (2), February, p. 40-44.

Tanner, J. (2004). "Receipt for Disaster Recovery," Telecomasia.net, [on-line] available at: www.telecomasia.net/telecomasia/article, article id:80300, 1 January 2004.

Toigo, J. W. (1989). *Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems,* Yourdon Press, Englewood Cliffs, NJ.

Turban, E., McLean, E., and Wetherbe, J., (2004). *Information Technology for Management, 4th edition,* John Wiley & Sons, Hoboken, NJ.

Vidal, R. (2002). "The New Risk Equation: How Companies are Planning for Disaster after 9/11/01," *Communications News,* February

Walch, D., (2004). "Apologetic Anemia in the Business Continuity Industry," *Disaster Recovery Journal,* 17 (3), Summer, pp. 72-73.

Washington State Department of Information Services, [on-line] viewed 10 August 2004, www.dis.wa.gov/pmframework/planning/riskmgmt.htm, © 2001 – 2004.

Woo, G., "Understanding Terrorism Risk," *Risk Management Solutions,* Jan. 2004, [on-line] viewed on 1 Aug. 2004, available at: www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf.