

A Case Study For Accounting Information Systems – A Business Continuity Plan For Protecting Critical Financial Information In The NYC Financial Services Industry

Mark D. Law, Bloomsburg University, USA

Gary Robson, Bloomsburg University, USA

ABSTRACT

This case study outlines a project launched by the Wall Street West organization, a data redundancy system in Northeastern Pennsylvania which provides backdrop for financial institutions located in New York City. The purpose of this study is threefold. First, the history on the importance of business continuity plans in a post 9/11 world is explored. Second, the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission recommendations regarding Disaster Recover, in addition to the requirements of The Sarbanes-Oxley Act, are reviewed. Lastly, an overview of Wall Street West's effort is provided, looking at some of the strategic advantages to locate in Northeastern Pennsylvania and demonstrating the important resources provided by Wall Street West to protect the nation's national security. Conclusions and case use recommendations are presented as this case is ideally suited for use in an Accounting Information Systems course at either the undergraduate or graduate level creating an awareness of the importance of business continuity planning.

Keywords: Backup Plans; Disaster Recovery; Accounting Information Systems

INTRODUCTION

The United States' financial services industry has and will continue to face many challenges over the prior and next decades. One of the most important challenges to be confronted will be planning for and responding to terrorism and natural disasters. No such challenge will be more taxing with which to deal and have such a profound and significant impact on the financial services industry as that of domestic and international terrorism. Significant events during the past 15 years exposed numerous problems for the United States financial services industry to consider and manage over the next decade and beyond. One important resource that has to be protected is the company's data. "Data is one of two irreplaceable corporate assets, second only to loss of life," writes Dennis Wenk (2004).

However, changes in technology may ease the burden of meeting some of these challenges - in particular, terrorists' actions - if proper planning is implemented. Companies must understand the threat and be proactive in responding to these types of activities. Planning, in the form of developing and instituting contingency plans to safeguard data, is instrumental in the companies' abilities to recover from devastating actions of terrorists. Companies that are not properly prepared for a terrorist attack are far less likely to continue as a going concern (Toigo, 1996). Wall Street West, a non-profit organization located in the Pocono Mountains of Northeastern Pennsylvania, has implemented a total backup solution for the financial service industry in New York City. An initiative of the Wall Street West Organization is to be a strategic pillar to New York City's financial industry by providing back-up, real-time replication, and data disaster recovery solutions for New York City's financial industry, strengthening New York City's status as the world's premier financial center (Wall Street, 2008).

HISTORY

The First Bombing of the World Trade Center

February 26, 1993 was an infamous milestone in United States history. Terrorists attacked the homeland of the United States marking the first major foreign terrorist attack on American soil. Until this attack, terrorism was thought of as an inherently foreign problem. In the lunch hour, Islamic terrorists detonated a 1,500 pound bomb, contained inside a truck, in the parking area below the World Trade Center. The results were deadly; six people were killed and hundreds of people injured from an explosion that ripped a five-story hole in the World Trade Center.

The bombing event seemed to disappear in the thoughts and minds of many Americans in the succeeding years. The stock market surprisingly brushed off the bombing as the market fell ½% the next day and climbed 13.7% over the subsequent year. However, a few experts in the financial services industry did not forget about the attack and remained concerned about the obsolescence of the industry's disaster recovery plans, which were designed primarily to withstand natural disasters and were no match for the human-induced destruction resulting from an international terrorist attack (Beachum & McManus, 2004). Unfortunately, the 1993 bombing was a harbinger of things to come as the U.S. financial services industry was a top target for terrorist attacks. As asserted, the United States homeland was struck on the morning of September 11, 2001 and financial services industry battered violently.

September 11, 2001 Attack on the Twin Towers

September 11, 2001 started out like most other days in New York City, but the impending events of that day would forever change a nation. At 8:46 AM a commercial jet, which many first thought was a small plane that had veered off course, crashed into the North Tower of the World Trade Center. The situation became more apparent when at 9:03 AM a second plane crashed into the South Tower. In a series of coordinated suicide attacks, four planes were hijacked by international terrorists with two planes crashing into the World Trade Center, one plane crashing into the Pentagon, and the last plane crashing into a field in southwest Pennsylvania (The 9-11, 2004).

Tragically, during the suicide attacks, an estimated 2,700 fatalities were reported in New York City—the exact number may never be known—and 125 fatalities at the Pentagon (The 9/11, 2004). The dreadful attacks and subsequent results of September 11, 2001 fulfilled the forecasts of professionals and experts involved in the financial services industry. The financial hub located in New York City was in jeopardy. The economic losses from the attacks were estimated to be in excess of 80 billion dollars. The financial services industry was hit hard from not only an economic standpoint but also a human capital perspective. Many firms were ill prepared to deal with the repercussion of a terrorist attack that destroyed both strategic economic assets and valuable personnel. Data and data systems recovery and continuity planning was reasonably well developed within the financial services industry as a whole, but it was implemented inconsistently by individual companies (Beachum & McManus, 2004). Many firms were not prepared well enough and were never able to overcome the events of September 11, 2001, and, subsequently, ceased business operations.

August 14, 2003 Blackout in NYC

On August 14, 2003, shortly after 4:00 PM, the New York City power grid was included in one of the largest electrical blackouts in U.S. history. The blackout crippled eight U.S. states and parts of southeastern Canada. The power outage lasted three days before power was finally restored (Miller, 2003). The blackout has faded from the memories of New Yorkers, but many questions still lingered within the financial services industry. The blackout stirred some controversy about the locations of remote backup systems. Anxious about business continuity, numerous New York-based financial firms developed back-up facilities in and around the New York metropolitan area. Some firms expected concerns about the distances necessary to achieve “full redundancy” in the wake of the 2003 blackout (Kite, 2003). Ironically, the results of the blackout focused attention on the need for geographically remote back-up systems rather than back-up systems located in the vicinity of the primary operations facilities for the financial services industry.

LESSONS LEARNED FROM THE FINANCIAL SERVICES INDUSTRY

Understanding the threat of terrorism, natural disasters, and unforeseen catastrophes is imperative. The above-mentioned events, coupled with many other significant activities, have left a profound effect on the U.S. financial services industry. An important lesson learned by the U.S. financial services industry during the past fifteen years is that a distinct possibility exists that unforeseen events may have an intense, negative impact on the industry without proper precautions. The timeline for events requiring business-continuity responses by U.S. companies has been amplified in the last five years. Ten events dictated full or partial relocations for U.S. companies, at home and abroad (Sandman, 2006).

Many financial services companies' backup and continuity plans were simply not sufficient in dealing with the magnitude of the recent events. These threats and peripheral issues started to transform thinking in the financial services industry. A salient discovery resulting from the effects of the 9/11 attacks was that the future of a financial super center - New York City - is reliant upon an excellent aggregate back-up plan to recover from such catastrophic events (Preimesburger, 2007). Business continuity planning, inclusive of aggregate backup plans and redundancy systems, is the key to business survival in the event of a disaster situation. The increased awareness of terrorism helped redefine the essential definition of a back-up system. Business continuity planning and disaster recovery are evolving and expanding. They not only encompass electrical power infrastructure, data backup and buildings to house systems and employees, but also include entire communities supplied with rail lines, educational facilities and all services necessary for financial enterprises to function (Sandman, 2006). In addressing some of the above-mentioned events in this paper, the U.S. government issued two significant publications on these subjects.

GOVERNMENT RECOMMENDATIONS

Interagency Government Report

In April 2003, three agencies - The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission - published the interagency paper titled "Interagency Paper on Sound Practices to Strengthen the Resilience of the United States Financial System." The paper contains three major business continuity objectives targeted at the financial services industry, coupled with four sound practice initiatives to ascertain whether the U.S. financial system has the ability to recover quickly from any impediments in a post 9/11 world (Interagency paper, 2003).

The U.S. financial market is a large, complex system composed of many related and interrelated subsystems. Due to this intricate and mutually supporting structure, all firms in the financial industry have a vested interest in enhancing the "overall resilience of the financial system." The goal of the agencies is to ensure, in a timely fashion, that crucial companies involved in financial markets are able to process and complete pending transactions and safeguard assets in the likelihood of a wide-scale disruption. The three business continuity objectives listed in the paper are:

1. Rapid recovery and timely resumption of critical operations following a wide-scale disruption.
2. Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location.
3. A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible. (Interagency paper, 2003)

In addition to the three business objectives, the agencies have listed four sound practice initiatives with the attention positioned on trying to lessen the impact of an interruption of the financial markets due to terrorist attacks or natural disasters. Business continuity planning, incorporating the four sound practices, is seen as the vehicle to help financial institutions diminish the effects of such attacks and disasters on the U.S. financial system. Business continuity planning is imperative for financial firms operating in today's post 9/11 business climate to prevent wide-scale outages and offer a sense of security. Significant back-up facilities, including back office functions, are at the center of the sound practices to ensure resumption of financial activities in time of peril. An important note should be made that the agencies are not recommending moving principal operations out of metropolitan areas. The four broad sound practices from the paper are:

1. Identify clearing and settlement activities in support of critical markets.
2. Determine appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets.
3. Maintain sufficient geographically dispersed resources to meet recovery and resumption activities.
4. Routinely use or test recovery and resumption arrangements. (Interagency paper, 2003)

SEC Guidelines

In April 2004, the Securities and Exchange Commission established rules for NASD and NYSE members to enact business continuity plans and procedural guidelines relating to unforeseen circumstances that may cause considerable business disruptions for members. According to SEC (2004), “the Commission believes it is important for securities firms to take concrete steps to strengthen their resilience and to address the continuing risks to the U.S. financial system posed by the post-September 11 environment. The recently-approved business continuity rules should help achieve that goal for individual firms and the securities industry as a whole.” Under the new rules, financial services firms should:

1. develop procedures related to significant business disruptions
2. develop business continuity plans
3. establish geographical diversity between primary and back-up sites
4. confirm back-up arrangements in recovering from a wide-scale disruption through testing (Business Continuity, 2003)

An important related development involving the NASD and NYSE members in regard to the above guidelines should be noted. Zuckerman et al. (2006) state, “On November 28, 2006, the National Association of Securities Dealers (NASD) and NYSE Group, Inc. (NYSE Group) announced the signing of a letter of intent to consolidate their member regulatory operations into a new self-regulatory organization (SRO). The plan is being hailed by securities professionals as a positive development which, if completed, will streamline and enhance consistency of regulatory efforts, eliminate conflicts under the current scheme of overlapping regulation, and result in regulatory cost savings for member firms.”

Sarbanes-Oxley Act

On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002 in response to accounting scandals involving a number of high profile corporations. The bill introduced a new age of corporate governance and a host of new regulations for corporations and accounting firms to follow with respect to the management and reporting of financial information. The Sarbanes-Oxley Act of 2002 plays an important role in business continuity planning and disaster recovery for corporations, even though it was not specifically mentioned in the Act (Berman, 2004; Hermanson et al., 2007). In particular, the Act indirectly provides for the inclusion of business continuity planning and disaster recovery through the interpretation and implementation of Section 404 Management Assessment of Internal Control as follows:

- (a) **RULES REQUIRED** - The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall
 - (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
 - (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
- (b) **INTERNAL CONTROL EVALUATION AND REPORTING** - With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement (Sarbanes-Oxley Act, 2002).

According to Berman (2004), “Section 404 of Sarbanes-Oxley mandates that organizations must understand the risks that may impact their financial reporting processes and which requires them to put in place the proper controls to deter financial misconduct. This is how business continuity became an inherent part of compliance.”

WALL STREET WEST

Wall Street West Overview

Wall Street West (WSW) is a \$40 million dollar enterprise whose main funding consisted of a \$15 million U.S. Department of Labor WIRED (Workforce Innovation in Economic Development) grant and more than \$25 million in federal, state, and private investments. WSW is a not-for-profit partnership comprised of over two dozen Northeastern Pennsylvania regional and Pennsylvania state-wide economic development agencies. In addition, the organization included private sector technology investment groups, workforce development organizations, area educational and research institutions, and other experts all having a stake in the project (Wall Street, 2008).

WSW resides in the Pocono Mountains of Northeastern Pennsylvania which has been long known as the “honeymoon capital of the world.” The Poconos are advertised as a romantic vacation getaway boasting natural scenic beauty, 150 lakes, resorts, and quaint, historic towns (Pocono Mountains, 2008; Goldstein, 2007). While the scenery and amenities remain, there has been a significant movement among politicians and business leaders to add to the current offerings of the Poconos Mountains. The additional contribution is to become the principal back-up center for New York City’s financial services industry by providing real-time replication and data disaster recovery for the critical financial operations of that industry in the event of a wide-scale system failure (Wall Street, 2008).

The Wall Street West System

There are two main initiatives of Wall Street West. The first is to provide business continuity services to New York City’s financial services industry by implementing a fully functional fiber optic network infrastructure connecting Lower Manhattan with Northeastern Pennsylvania. Wall Street West enabled back office functions for the financial services industry located in New York City in Northeastern Pennsylvania. The project empowered redundant, instantaneous data transmission between the two areas and, in addition, provides business continuity, recovery, and data replication for the New York City financial services industry.

The second initiative is to support education in area colleges and universities through grants, other support services, and to promote workforce education and development in the region. Wall Street West incorporates long-term strategic plans to prime workers for high-skill, high-wage career pathways and to meet the future employee competencies needed in the financial sector and related information technology arena. In this regard, Wall Street studied which skills were required by financial companies, reviewed the area’s worker training programs, appraised area college and university curriculums, and identified areas that needed to be improved (Wall Street, 2008).

This paper concentrates on the first initiative discussed above and the nucleus of the Wall Street West project - the fiber optic network - the backbone of the Wall Street West project. Wall Street West utilizes synchronous data replication which replicates data at a remote site; in this case, Northeastern Pennsylvania.

The Wall Street West’s Strategic Advantage

One of the main reasons Northeastern Pennsylvania was chosen as the business continuity site was the strategic location of the area. First and foremost, the nine counties of Northeastern Pennsylvania region fall within the 125-mile limit (in each direction) required for synchronous signal transmission, as discussed above, making the Wall Street West region strategically located to New York City.

Secondly, the region was in compliance with all of the Federal Regulatory Agency recommendations regarding geographical diversity between the primary site of New York City and the back-up site Wall Street West. Listed below are the long-standing principles of business continuity planning that WSW is in conformity with:

1. A separate transportation system from New York City.
2. A separate telecommunications system from New York City.
3. A separate electric power grid from New York City.
4. A separate watershed from New York City.
5. A separate nuclear impulse from New York City (Wall Street, 2008).

Lastly, a developing trend in the last twenty years has seen many firms from larger metropolitan areas in the financial services and insurance industry established divisions of their operations in the WSW region. Currently, over 25,000 residents work in these industries in Northeastern Pennsylvania (Northeast Pennsylvania). The primary reason for these moves was the same benefits WSW had to offer in business continuity services. Listed below is a summary of the unique benefits of the WSW region:

1. centrally located with easy access to NYC, Philadelphia, and Washington DC
2. well-developed telecommunications infrastructure
3. well-educated workforce
4. affordable energy costs
5. substantial tax incentives for businesses
6. wide availability of open commercial sites and industrial parks
7. efficient workforce with lower operating costs than major cities (Wall Street, 2008)

CONCLUSIONS

One of the many ramifications of 9/11 and other recent disasters was a need for more efficient and effective disaster recovery sites. According to the Interagency paper (2003), the business continuity planning process should take into consideration improvements in technology and business processes supporting back-up arrangements and the need to ensure greater resilience in the event of a wide-scale disruption. Currently, many of the larger financial services firms in New York City are using areas located in the vicinity of New York City for the business continuity and disaster recovery plans. However, many of these areas do not meet the recommendations of the Federal Regulatory Agency regarding geographical diversity of backup facilities.

The Wall Street West project looked to provide a proactive solution to this problem. The stakeholders of Wall Street West envision a real-time replication and data disaster recovery system located in the Pocono Mountains to serve as a back drop for New York City's financial services industry. In the Wall Street West vision, the traditional Pocono Mountains activities of skiing, boating, hiking, etc. would be juxtaposed to the latest fiber optic technology and critical financial information in an ever-shaping new millennium. Even though Wall Street West had presented a foundation for many firms for their disaster recovery site, they still had to sell the benefits of their services to financial services firms, and, currently, this sell is harder than some predicted as WSW has not yet become the principal back-up center for New York City's financial services industry.

CASE USE RECOMMENDATIONS

This case study is ideally suited for use in an Accounting Information Systems course at either the undergraduate or graduate level. The case can be used as a student assignment, individual or group, or a classroom example. As a classroom example, relevant aspects can be investigated by the students either prior to or during class. Possible requirements would include listing the criteria necessary for a desirable data redundancy system. The attributes of Wall Street West can be investigated and evaluated for the effectiveness in satisfying each criterion. Finally, students can conjecture as to why Wall Street West number of clients has not lived up to expectations.

AUTHOR INFORMATION

Dr. Mark Law is an Associate Professor of Accounting at Bloomsburg University of Pennsylvania. He received his Ph.D. from the Pennsylvania State University and is a licensed Certified Public Accountant. His career began in public accounting as a staff accountant before he established and developed an accounting and computer consulting

practice prior to moving into academia. His research interests include the areas of accounting information systems, construction technology, and emotional intelligence. E-mail: mLaw@bloomu.edu (Corresponding author)

Gary S. Robson is an Associate Professor and Accounting Department Chair at Bloomsburg University of Pennsylvania. He received his Accounting Ph.D. from the University of Arizona. His career as a divisional manager in the steel industry has given him a distinctly user-oriented perspective from which he teaches graduate and undergraduate management accounting. He has published articles in numerous journals, including *Academy of Management Journal*, *Research in Accounting Regulation*, *CPA Journal*, *Catalyst*, *Journal of Private Enterprise*, and others. E-mail: grobson@bloomu.edu

REFERENCES

1. Beachum, A. E., & McManus, D. J. (2004). Recovery of financial services firms in the World Trade Center, Post 9/11/01. *Information Systems Security*, May/June 2004, 46-55.
2. Berman, A. (2004). Business continuity in a Sarbanes-Oxley world. How business is leveraging business continuity to comply with the new regulation. *Disaster Recovery Journal*, 17(2).
3. Business continuity planning for trading markets, (2003, September 25). U.S. Securities and Exchange Commission. (Release No. 34-48545; File No. S7-17-03).
4. Goldstein, M., (2007, May 21). Wall Street in the poconos. *Business Week*, 4035, 13.
5. Hermanson, D. R., Ivancevich, D. M., & Ivancevich, S. H. (2007). Disaster recovery planning: What Section 404 audits reveal. *CPA Journal*, 77(12).
6. Interagency Paper on Sound Practices to Strengthen the Resilience of the United States Financial System, (2003, April, 7). U.S. Securities and Exchange Commission. (Release No. 34-47638; File No. S7-32-02).
7. Kite, S., (2003). Firms look close to home for backup. *Securities Industry News*, 15(35), 1-21.
8. Miller, P. (2003, October). Surviving the blackout of 2003. *Catalog Age*, p. 16
9. Northeast Pennsylvania: Resource profile for financial services and insurance companies, (2007). Retrieved April 12, 2008 from http://www.pennsnortheast.com/v3/downloads/msb_study.pdf
10. Pocono mountains. (2008). Retrieved April 29, 2008 from <http://www.800poconos.com/>
11. Preimesberger, C. (2007, September, 24). Backing up Wall Street's IT. *Week*, p. 31
12. Sarbanes-Oxley Act of 2002. (2002, July 24). 107th Congress report 2nd session, House of Representatives. (Report 107-610).
13. Sandman, J. (2006, November 6, Special Report). Congressman says west is best for disaster sites. *Securities Industry News*, 15(35), 1-21.
14. SEC approves NASD and NYSE business continuity rules. (2004). Retrieved April 22, 2008 from <http://www.sec.gov/news/press/2004-53.htm>
15. The 9-11 commission report final report of the national commission on terrorist attacks upon the United States, (2004). Official Government Edition Superintendent of Documents, U.S. Government Printing Office, Washington, DC.
16. Toigo, J. (1996). *Disaster recovery planning for computers and communications resources*. New York: John Wiley & Sons.
17. Wall Street West. (2008). Retrieved April 28, 2008 from <http://www.wallstreetwest.org>
18. Wenk, D. (2004). Is 'good enough' storage good enough for compliance? *Disaster Recovery Journal*, Winter 2004.
19. Zuckerman, J. R., Landy, C. J., Hyatt, C. C., & Molin, D. Z., (2006, November, 30). *NASD and NYSE member regulatory operations to merge*. Client Alert. Retrieved April 28, 2008 from <http://www.pillsburylaw.com/LawPortal/ep/entrance.do>

NOTES