

Recovering from Database Recovery: Case Studies and the Lessons They Teach

Mary J. Hoferek, *Member, IEEE*, and Susan C. Wilson*

Abstract—The attacks of September 11, 2001 and Hurricane Katrina forced database professionals to truly reconsider what it means to recover a database. Recovering the data stored on the disks is just one part of recovery. Reassessing disaster recovery plans and preparing to recover again is another. Perhaps the two most important changes include 1) addressing the needs of people in the recovery plan and 2) viewing database recovery from an enterprise-wide perspective, rather than from a technology slant. This paper discusses two major events that force us to think about recovering from database recovery.

Index Terms—Disaster Recovery, Database Recovery, Information Valuation, Intellectual Assets, Knowledge Management.

I. INTRODUCTION

Two major events forced database professionals into recovery mode. The attacks of September 11, 2001 and the devastation caused by Hurricane Katrina destroyed data centers and cost employee lives. Those events forced a thorough re-evaluation of disaster recovery plans within industry, and forced systems professionals to implement new levels of backup and recovery planning and execution. As disaster plans are reassessed and re-crafted for robust future implementation, they reflect the many important lessons learned from those who survived and recovered. This paper examines several case studies of organizations affected by the September 11 attacks and Hurricane Katrina, gives an assessment of the cost of losing data and staff, and suggests disaster aversion and mitigation actions for the future.

II. CASE STUDIES

These case studies illustrate the effects of total devastation on three major and venerable organizations: one a global capital investment player, one a risk management and insurance house, one a respected American university. Each had crafted excellent risk management and disaster recovery

plans that were in accordance with industry best practices. Each planned for emergencies of a magnitude that was entirely within the realm of the possible. None expected the swift and brutal destruction of such unimaginable order. But each responded with deliberated reason. Each survived. And each learned extraordinary lessons that serve industry at large.

The attacks of September 11, 2001 provided no warning. Two companies, Barclays Capital and Putnam Investments learned some hard lessons that day. Wall Street and its financial institutions were reminded about the importance of disaster recovery sites [6].

With Hurricane Katrina, the Gulf Coast had some warning. But it was neither timely nor precise. Even the best risk and disaster management strategies could not mitigate the unavoidable breaches in communication and disruption of leadership that Tulane University suffered.

1) Barclays Capital

Barclays Capital is an international investment bank; its New York office was located at 222 Broadway, less than a mile from the World Trade Center (WTC). After the first tower was hit on September 11, the leadership implemented Phase 1 of the firm's disaster response plan. This required employees to report to a staging center at the WTC. On this dreadful day, however, the assembly site was changed to the area toward the seaport [5].

When second plane hit, Phase 2 of their disaster response plan went into effect. This included a call to disaster recovery vendor Comdisco in N.J. However, damaged phone lines made calls out of New York City challenging. The Barclays staff decided to send an e-mail and "put someone in a car and go there," if nothing else worked. Comdisco received the e-mail and the declaration of disaster was accepted. The disaster recovery plan called for the Comdisco site to receive about 1/3 of Barclays 1,200 employees and support them for 2 days through 2 weeks, if necessary. If staff could not return to their offices after two weeks, the Barclays' plan dictated that they find longer-term space to continue operations [5].

While Phase 2 was in process, Barclays' Chief Information Officer was finally able to reach the firm's London office and establish a command-and-control center there. Employees were able to call that center by 9:30 a.m. Since employees were unable to travel from Manhattan to the backup site, a local command-and-control center was setup at an employee's home on East 56th Street. Around 2:00 p.m., employees started arriving at the backup facility in N.J. They started set-

Manuscript received March 7, 2007. This work was supported in part by the University of Maryland University College and PTG International, Inc.

Mary J. Hoferek, Ph.D. is with the University of Maryland University College, Adelphi, MD 20783 USA (phone: 301-985-4602; e-mail: mhoferek@umuc.edu, mary.hoferek@gmail.com).

Susan C. Wilson is with PTG International, Inc. Germantown, MD, 20874, USA. (e-mail: swilson1958@hotmail.com).

* © Copyright 2007, Hoferek and Wilson. This material may not be used or reproduced in any form without written consent of the lead author

ting up desktops and establishing connectivity with their critical business partners. By 4:00 p.m., most employees had been contacted and told where to go the next day. By daybreak, critical applications for “funding, money transfer, government trading and derivatives” were restored and operational [5].

2) *Marsh & McLennan/Putnam Investments*

Marsh & McLennan was not as fortunate as Barclays on September 11. Marsh, an insurance brokerage firm, lost almost 300 people and its entire data center. However, it had a “sister” arrangement with Boston-based Putnam Investments. Marsh and Putnam are independent companies, and while they had set agreements in place, the Putnam technical staff had little functional knowledge of Marsh’s systems and environments, and was thus hampered in their efforts to restore Marsh to operational. Putnam needed about four business days to recover Marsh’s critical systems [6].

To a financial house, four days of lost work in the global market can be devastating. Upon review, Putnam Investments determined that it could have returned to operational within 4-6 hours at its remote site but for all its skill, the incoming team did not have site knowledge of Marsh’s infrastructure, and had no procedures to work from. The net loss to the company for the four days was incalculable but was estimated by Marsh in the range of roughly \$1 billion for lost revenue, and \$187 million to recovery [10]. The replacement cost of infrastructure was minimal. The replacement cost of the people and their knowledge is incalculable. However, at the risk of heartlessness, had Marsh included identifying and valuing intellectual assets as a line item with physical assets, that figure may have been possible to determine.

3) *Tulane University*

On August 25 2005, Tulane University administrators heard rumors that Hurricane Katrina was on the way, but then it looked as if it might head for the Florida panhandle. The next day, August 26, they decided to put their hurricane response plan into effect. On August 27, they evacuated their students, by previous agreement, to Jackson State University. A skeleton crew was setup on site at Tulane. On Sunday, August 28, Katrina was declared a Category 5 hurricane and Tulane brought down all of their information systems; the backup tapes were left in the data center. At 11:00 p.m., the evacuation of the uptown campus was completed, except for the President, Chief Financial Officer, and a few other staff members. More people stayed at the downtown campus because the medical center had patients. Katrina made landfall as a Category 4 hurricane on August 29. Tulane suffered major wind damage, but the buildings withstood the force and remained structurally intact [7].

Rumors started to circulate about failing levees; water started to fill the back half of the uptown campus and in the downtown campus by late Monday (August 29). August 30 and 31 were spent trying to evacuate remaining personnel. The disaster plan called for the senior administrators to stay on the campus. This action left them stranded on the second

floor of a building on a flooded campus without food, electricity, sewer, or a reliable communication system. This cost precious recovery time as the senior administrators sought to survive rather than help their institution recover [2]. It became critical to try to get the President and the Chief Financial Officer out. Several attempts to evacuate them failed. Finally, they used a cherry picker to get them to dry land where they hot-wired a cart to traverse a levee to a spot where a helicopter could pick them up. The helicopter took them to the airport where they were flown to Houston [7]. Houston had not been designated as a backup site for a command center and it was just by chance that the “recovery” administration found themselves there. Once the team started to function, they needed to figure out how to contact their 6,000 employees. They set up a website and asked employees to register their contact information; at this point, traditional methods of communication – telephones, cell phones, and computer communication – did not work. Text messaging was the only reliable means to contact each other [2]. Approximately three weeks later they evacuated Houston and went to Dallas to avoid Hurricane Rita. On September 25, they returned to Houston where Tulane had already had a presence. Soon after, they returned to New Orleans [7].

While the administration of Tulane was attempting to establish a viable command center, the IT staff was attempting to recover the backup tapes [13]. The center did not have a remote site to store their backup tapes [2]. The data center was on the 14th floor of a high-rise near the Superdome and was not water damaged, but lost all power. On the first attempt to get the tapes, the staff found themselves locked out and unable to gain entry to the building. Several days later, the IT staff slogged through the dark, hot building to get to the backup tapes so they could restore critical systems. After the storm, Tulane hired SunGuard, of Voorhees, N.J., to load its student information system and financial applications onto a mainframe so they could restore basic functions [13]. Through all of this, Tulane did not miss a single payroll [8].

III. LESSONS LEARNED AND IMPLICATIONS FOR THE FUTURE

A key part of recovery is logging the painful but necessary lessons learned. While tested beyond an unimaginable benchmark, industry can benefit through a deeper and broader range of planning and preparing. Two lessons in particular can be taken to heart:

- Plan for total devastation. Consider every aspect of the organization’s infrastructure, systems, data, staffing, suppliers, and agreements in terms of what would happen to the organization if any one or all of these critical elements was breached or destroyed. For database professionals, this entails a significant realignment of their roles from performing highly technical, tactical work to taking their seats at the strategic planning table.
- People and their knowledge are the most valuable assets to an organization and the only real key to

recovery. As such, they must be protected, valued, and their knowledge inventoried and insured, both in day-to-day operations and during recovery. DBAs must be proactive in identifying and quantifying the value of their own intellectual assets.

The lessons learned from the experiences of Barclays Capital, Marsh & McLennan/Putnam Investments, and Tulane University were reported from their sources. They are consistent with industry's best practices in this post-September 11, high-stakes world.

A. Physical Separation

In response to the September 11 attacks, several financial institutions have invested heavily in redundant data centers. Putnam Investments, Mellon Financial Corporation, and John A. Levin & Company now have two data centers each that are physically separated, although they follow slightly different protocols for data backup and storage. Some of the centers provide synchronous data replication. Another takes full data dumps daily for non-sensitive data and has implemented real-time replication for its most sensitive data. Putnam has two data centers located 70 miles apart outside Boston. Each is outfitted with clusters and sophisticated platforms that accommodate events such as disk failures and power outages. The data centers are connected through self-healing, high availability fiber networks. If one data center is lost, the other data center will seamlessly support all of the business needs. As another layer of protection, Putnam takes backups to tapes which are stored offsite in a bunker. Putnam has a contract for recovery services out of the region with a service provider. The costs for backup sites and recovery capabilities are enormous investments for the financial institutions [6], but may mean the difference between survival and bankruptcy.

Redundant data centers provide an alternative strategy. Advocates maintain that rather than one backup site, redundant data centers throughout the country would be a better alternative by providing distributed data protection sites. This approach has been adopted by many Internet companies [1].

B. Ergonomics and Mobility

While financial institutions have been developing backup sites, the authors could argue that only backups are insufficient to prevail in a disaster. Excellent disaster recovery plans were not adequate on September 11. While backup sites were available, recovery was hampered by insufficient hardware, outdated software, inadequate database backups, and in a few cases, systems that worked in isolation rather than an integrated system that allowed users to work effectively [1]. And without adequate identification of the elusive intellectual skills necessary to implement restoration under duress, those people who are lost, indisposed, or unreachable will prove to be the greatest lost key to recovery.

In addition, disaster recovery plans had underestimated the number of people needed to resume operations. In some cases, fewer than half the required desks were available for

operations to resume. Most trading systems took days and in some cases, weeks to restore operations, sustaining devastating losses of business. A major cause of interruption of service was lack of attention to workflow. For example, in addition to identifying physical and intellectual assets and how they are to be safeguarded, disaster recovery planning must capture the logistics of stationing key people to oversee and execute mission critical activities, and how these people and activities interact with each other.

Disaster recovery plans need to account for both database backups and workflow management. Whether in-house or at an external site, work spaces and environments need to be setup for mobility and flexibility. When users arrive at the site, they need to be productive immediately. Key tactics to assure this are rehearsed recoveries, interchangeable/interoperable hardware, and a physical and logical recovery infrastructure based on a plug-and-play model [1].

C. Use of the Web

The World Wide Web is an ideal tool for disaster recovery. It can be accessed with a minimum of installation and from any desk. However, most financial systems do not have a web interface. In the event of a disaster, however, a scaled-down version of a system would allow a business to continue productively. Employees could use preconfigured laptops from their homes, hotel rooms, or backup sites to continue essential operations [1].

The Internet was used by many universities in the wake of Hurricane Katrina. Emergency off-campus websites were used to keep their students, faculty, and staff informed. The outage of cell phones, Blackberries, and other communication devices kept many people walled off from Internet-delivered information, but for those with connectivity, it helped people find out if they were going to get paid, or if classes were going to be held, etc. The Internet also helped students and professors connect with and support each other [4].

Other institutions set up websites to help affected universities. They posted announcements from the institutions, helped people get in touch with each other, and hosted online courses. Students and professors also set up blogs to help everyone connect and to provide information. One Tulane student had a blog that had 13,000 page views in the first two days [4].

D. Other Communication

In a disaster, it is imperative to ensure that communications survive. After Hurricane Katrina hit, telephone lines fell and cell phones were inoperable. In response, some institutions have distributed satellite phones to all administrators [9]. Tulane set up a temporary e-mail address from the Houston site; more than 3,000 messages were received during the first days. Based on those messages, the temporary website was updated with common questions and answers [4].

Some lessons can be learned from the Barclays team. One particular strength was their "triangulated network" – the

office in New York, a backup site in N.J., and the firm's headquarters in London. They had multiple telecom providers; when they lost one, they could use the other. Barclays found that it was hard to reestablish connections with business partners because they were also in disaster recovery mode; emergency contact phone numbers were hard to find. Barclays learned that they need increased bandwidth between N.Y. and London in case they have to exchange large amounts of data quickly [5].

E. Care for People

The stress level of people working through a disaster to bring about recovery is incalculable. But those people, and the care and knowledge they hold, are the critical path to survival. Assume that while they are focused on restoring the organization to operational state, they will be distracted by concern for their families, fear for their personal safety, chilling fatigue, and disoriented from trauma. The authors believe that how those people will be nurtured during recovery must be carefully planned out in a disaster recovery plan.

Under such stress, simple mundane tasks bring about grounding and a reminder of life outside of the disaster. Taking time out to walk the dog, watch a hockey game, nibble a snack in the quiet of a favorite or inspirational missive, or just stand down for a break can refresh a responder to a focused, level-headed state of mind. This reduces the conditions that enable misjudgment and errors, and cares for those who are caring for the organization [11].

In a disaster, key staff members may be unavailable or family members may be unaccounted for. The disaster recovery plan should prepare contingencies for caring for staff not only to fill in for their colleagues, but to handle the trauma of losing a trusted and critical staff member [11].

Systems can be restored or rebuilt. Not always so for people. They must be put first. Plan strategies to minimize, even automate their responsibilities. For example, to continue payroll and accounts payable operations, set up credit cards and direct deposit to avoid printing checks [8].

F. Identify Critical Knowledge

The real value of intellectual assets is generally felt only in their absence. When key knowledge – the tacit understanding of how things get done in an organization and what that organization knows – is breached, the chances for recovery are compromised. This knowledge drives strategic decision making and it is the most valuable asset that will get an organization back on its feet [12].

Knowledge exists in an organization as explicit – written down, formally communicated – in the forms of inventories, job descriptions, customer records, product documentation, to name a few good sources. Implicit knowledge has the greatest longstanding value to the organization and is, by and large, intangible. These invisible assets include historical knowledge of the organization's processes, capacity for innovation, position in the market, unwritten assessments of customers

and suppliers, reputation, informal channels of information flow, and institutional memories. In short, these are the assets that restore the organization's true value in ways that servers and desks cannot.

The authors believe that capturing that knowledge in the forms of knowledge maps, video-recorded interviews, and intellectual inventories (similar to a physical inventory sheet) is the first step in planning to restore the organization. This information should be safeguarded with the same care shown to data and servers. For database professionals, this is likely a new consideration. In crafting response and recovery plans, IT workers should routinely ask the very sobering question, "If I cannot do my job, what would someone need to know to do it?" This charges IT workers to view themselves and their counterparts as true designers of the strategic mission; their tactical effort is proactively itemizing what they know to meet that strategy.

After identifying mission-critical knowledge, where it resides, and capturing that information, assign values to it. Several models for information valuation are available, each taking into account different data points about human capital, customer relationships, and structural capital. A very simple high-level model to determine an organization's total value is to subtract its book value from its market value. The difference, it can be argued, is its intellectual value. Usually this is a very sobering figure [12].

A common metric is that the value of an organization's intellectual capital is roughly 5-10 times that of its physical assets [3]. Buildings and books can be replaced. Once the critical knowledge that sustains and grows the organization is gone, that key asset is gone forever.

G. Nuts and Bolts

These points are well-documented in risk management best practices but their importance was underscored by the recovery activities of Barclays, Marsh/Putnam, and Tulane. The authors believe these are imperative tasks in planning for recovery from disaster.

Write a comprehensive risk management plan. Though the consequences are difficult to consider, ask the tough questions, and list mitigation and aversion strategies. For example, if a university cannot provide classes, can the institution survive? Consider how long a financial house can be absent from the global market before it collapses. Identify the key people in the organization, what makes them key, and what the organization would do if they were unavailable.

Having a disaster recovery plan is critical. Testing and exercising it with an enterprise-wide team is imperative. Be sure everyone can access it, especially under compromised circumstances.

Establish a command and control center, and an alternative. Set up mutual agreements with other institutions to provide and share a command and control center.

Set up facilities for displaced staff, students, and faculty. After Hurricane Katrina, each person on staff had to decide on

their own where to go. Establish mutual aid agreements ahead of time, and inform staff where they can go for help.

When itemizing physical assets in insurance logs and risk management plans, identify and itemize the organization's intellect assets as well. Determine the value of the knowledge by answering the question "How much will it cost to replace what this key person knows?"

Review insurance coverage and contracts. Likewise, look at vendor contracts to protect against price gouging and provision for support. Also, verify that vendors' disaster recovery plans are sufficient to predict that the vendors will likely be able to survive to support its clients [9].

For disaster recovery, consider four P's and an A: planning, preparation, assessment, process, and people [7]. Tulane University had a disaster response plan for hurricanes. A formal disaster recovery plan, however, was assessed at \$300,000 and Tulane wasn't able to afford it.

Prepare for possible disaster. Test communication systems and have a plan for people so they go to one place. As a point of process, communicate, communicate, communicate. Be sensitive to people [8].

H. Plan for Total Devastation

If data and static information are the bricks of an organization, its knowledge is both its foundation and mortar. This knowledge, held by people, is even more valuable than the total of its physical assets. It is much more fragile. A data server destroyed can be replaced. Critical information held in a person's brain cannot.

Every aspect of an organization's risk management strategy should map to the organization's strategic goals. In crafting such a strategy, risk identification, mitigation, and aversion methods should be based on these questions:

- "What would happen to my organization if my key people could not help us recover?" This requires that the organization identify who is key, and what knowledge they have that makes them invaluable.
- "How much can the organization afford to lose? What is its 'bottom line' from which it cannot recover?" This refers not just to dollars and cents but to provision of service, discontinuity of operations, or loss of a market share.
- "In case of total devastation, which organizational units must be restored first? What is required – in time, money, people, tools, and assets – to do so." Determine the dependencies of the different units on an enterprise-wide level, not just within a department.

These are very difficult questions to ask. They are even harder to answer. But for an organization to recover and possibly thrive, planning for the worst-case scenario will help protect its people and its mission.

IV. CONCLUSION

From the devastation of September 11 and Hurricane

Katrina, the authors conclude that these case studies instill the need for database professionals to expand the concept of database recovery from stove-piped activity to an enterprise-wide mission. Database professionals are typically trained to restore the hardware and software of a system, particularly the database instance and the data. Technical recovery alone is no longer sufficient. Restoring the information on the disks is only one part of a complex system of recovery. Database professionals need to know the broader aspects of recovery and explore their role in the entire organization's disaster recovery mission. This lays fertile ground for database professionals to develop innovative, technical preparations for disaster recovery. We have learned sobering lessons from those who survived these two terrible events.

V. REFERENCES

- [1] Aurora, N. (2002). If the Unthinkable Happens. *Wall Street and Technology On-Line*. March 8, 2002. Retrieved October 9, 2006 from <http://www.wallstreetandtech.com/showArticle.jhtml?sessionId=0NRTY SK3YRPQYQSNLPCCKH0CJUNN2JVN?articleID=14703631>.
- [2] Cowen, S. S. (2006). After Katrina: Two Presidents Reflect. *The Chronicle of Higher Education*, 52:33, p. B12, April 21, 2006. Retrieved February 27, 2007 from <http://chronicle.com/weekly/v52/i33/33b01201.htm>.
- [3] David Skyrme Associates (n. d.). *Measuring the Value of Knowledge*. Summarized on <http://www.skyrme.com/kshop/kbriefs.htm#Measures>.
- [4] Foster, A. L. & Young, J. R. (2005). The Internet as Emergency Tool. *The Chronicle of Higher Education*, 52:4, p. A39, September 16, 2005. Retrieved September 27, 2006 from <http://chronicle.com/weekly/v52/i04/04a0391.htm>.
- [5] Guerra, A. (2001). Disaster Recovery in Action: Barclays Capital. *Wall Street and Technology*. October 8, 2001. Retrieved October 9, 2006 from <http://www.wallstreetandtech.com/showArticle.jhtml?sessionId=0NRTY SK3YRPQYQSNLPCCKH0CJUNN2JVN?articleID=14703631>.
- [6] Kramer, L. (2005). Always Be Prepared. *Wall Street and Technology*. August 22, 2005. Retrieved October 9, 2006. from <http://www.wallstreetandtech.com/features/showArticle.jhtml?articleID=169500473>.
- [7] Lawson, J. (2005a). Hurricane Katrina and Tulane U. A Look Back at a Disaster Plan: What Went Wrong and Right. *The Chronicle of Higher Education*, 52:16, p. B20. December 9, 2005b. Retried September 27, 2006 from <http://chronicle.com/weekly/v52/i16/16b02001.htm>.
- [8] Lawson, J. (2005b). Katrina and Tulane: a Timeline. *The Chronicle of Higher Education*, 52:16, p. B21, December 9, 2005. Retrieved February 27, 2007 from <http://chronicle.com/weekly/v52/i16/16b02101.htm>.
- [9] Lipka, S. (2005). After Katrina, Colleges Nationwide Take a Fresh Look at Disaster Plans. *The Chronicle of Higher Education*, 52:8, p. A28. October 14, 2005. Retrieved September 27, 2006 from <http://chronicle.com/weekly/v52/i08/08a02802.htm>.
- [10] Marsh & McLennan (2002). Annual Report, 2001. Available from http://www.mmc.com/investors/AnnualReport_01.pdf.
- [11] Selingo, J. (2005). Putting a University Back Together. *The Chronicle of Higher Education*, 52:4, p. A18. September 16, 2005.
- [12] Sveiby, K. E. (1998). *Measuring Intangibles and Intellectual Capital - An Emerging First Standard*. Available from <http://sveiby.com/Portals/0/articles/EmergingStandard.html>.
- [13] Thibodeau, P. & Mearian, L. (2005). After Katrina, users start to weigh long-term IT issues. *ComputerWorld*. September 15, 2005. Retrieved January 16, 2007 from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=104542&intsrc=article_pots_bot.