Dispelling 10 Common Disaster Recovery Myths: Lessons Learned from Hurricane Katrina and Other Disasters

BRETT J. L. LANDRY
University of Dallas
AND
M. SCOTT KOGER
Western Carolina University

Disasters happen all the time; yet despite this, many organizations are caught unprepared or make unrealistic assumptions. These factors create environments that will fail during a disaster. Most information technology (IT) curricula do not cover disaster recovery (DR) plans and strategies in depth. The unfortunate result is that most new computer systems are implemented without sufficient disaster recovery plans and testing. Courses on network security need to examine DR as a real threat and cover it as a core module. By dispelling the 10 common myths, organizations can better plan, develop, and test true DR plans.

Categories and Subject Descriptors: C.0 **[Computer Systems Organization]**: General -- *Systems architecture*; C.2.1 **[Computer-Communication Networks]**: Network Architecture and Design; C.2.0 **[Computer-Communication Networks]**: General -- *Security and protection*; K.0 [**Computing Milieux**]: General; K.3.1 **[Computers and Education]**: Computer Uses in Education -- *Computer-assisted instruction*; K.3.2 **[Computers and Education]**: Computer Science Education – *Curriculum*

General Terms: Experimentation, Human Factors, Reliability, Security

Additional Key Words and Phrases: Hardware failures, software failures, backups, network attacks, viruses, worms, business continuity, disaster recovery, IT curricula

1. INTRODUCTION

Disasters happen all the time; yet many organizations are caught unprepared or make unrealistic assumptions. Some organizations are severely affected by disasters because they fail to plan and test effectively. These factors create environments that will fail during a disaster. However, most information technology (IT) curricula do not cover disaster recovery (DR) plans and strategies in depth. The unfortunate result is that most entry-level IT workers implement new computer systems without sufficient disaster recovery planning and testing. Network security classes need to examine DR as a real threat to network security and cover it as module and not just a topic to be glanced over lightly. By dispelling 10 common myths, organizations can better plan, develop, and test true DR plans.

Authors' addresses: Brett J.L. Landry, Graduate School of Management, University of Dallas, 1845 East Northgate, Irving, TX ; email: blandry@gsm.udallas.edu , M. Scott Koger, Information Technology, Western Carolina University, Forsyth B-12, Cullowhee, NC 28723; email: skoger@email.wcu.edu

2. WHY IS DISASTER RECOVERY EDUCATION IMPORTANT?

Pessimists are not surprised when disasters strike because disasters do actually happen, all the time. Even the most unlikely scenarios will occur at some point. One likely scenario is that a tree will fall on a power line during a thunderstorm. The chance that the utility pole will catch on fire in the rain is unlikely; but if it does would the fire department be able to extinguish the fire while the lines remain energized? Even more unlikely is that minutes after the burning utility pole loses power, the uninterrupted power supply (UPS), intended to supply power to the server room during an outage, fails because the roof is leaking water through the UPS. The consequence is that all servers, networks, and related equipment are shut down incorrectly. But such was the unfortunate case at a southeastern university in April 2004. There are a number of issues and questions that need to be planned for and implemented prior to such a disaster: What will the consequences be upon start-up? Will the data remain intact? Will back-ups be needed? Will the back-ups be valid? In light of Hurricane Katrina, organizations must consider disasters as larger issues and look beyond the single event. What will the post-disaster business environment look like? What will the civil restrictions on entering the area be? These are questions that must be addressed and considered for successful DR plans.

Hurricane Katrina has demonstrated the need for successful DR plans. No one expected when they were evacuated that it would be weeks before they could get back into the metro New Orleans area; no one expected that homes and businesses would be under saltwater for weeks due to levee breaches; no one expected that areas that had never been flooded would be because due to decisions that allowed pumping stations to shut down during the storm, and remain off after the storm, causing massive flooding in areas unaffected by breaches in the levees; and no one expected that municipal web sites would remain offline because they did not have a DR plan. Many emergency response efforts were crippled by the lack of back-up or alternate communications. How can managers contact their staff to coordinate a response if company networks, e-mail servers, and even the public phone networks are knocked out?

As companies continue to use IT as a core function of their business, there needs to be a clear understanding of what will happen to the organization if IT resources become unavailable. Responsible management requires an objective evaluation of all potential physical threats, and a comprehensive plan to deal with them. There are a variety of disasters to account for, including natural disasters, power issues, and environmental issues: (i.e., heating, cooling, and humidity control), software problems, virus and worms, external attacks, and internal employee attacks.

In the Katrina example, what should companies do if they cannot get to their facilities for weeks or months? Current back-up tapes that survived the initial storm and were above the waterline in flooded buildings were often damaged by remaining in humid, moldy environments for weeks before the city was reopened to civilians. Servers and network equipment undamaged by the initial effects of the storm were damaged by sitting for weeks in flooded buildings without air-conditioning. Can businesses, suppliers, and customers survive being unplugged for weeks? For organizations that have tightly integrated supply chains, the disaster plan, or lack thereof, will affect everybody in the supply chain. When a public utility has no DR plan, none of the organizations that were counting on it to provide a stable environment as part of their DR plan can get on with the business of recovery. Public and private interest are intertwined in our economy – without sewers, water, drainage, public-order provided by law enforcement, and especially levees, the DR plans for all but the most foresighted organizations in New

Orleans were inadequate. The four hurricanes that hit Florida in 2004, the tsunami that impacted 14 nations in December 2004, and the devastation left in the wake of Hurricanes Katrina and Rita should put everyone on notice. It's not a question of if, but when, a disaster will strike. Can any organization afford not to have a DR plan? What are the costs of losing everything?

In 2003, the Federal Reserve System, the U.S. Department of the Treasury's Office of the Comptroller of the Currency, and the U.S. Securities and Exchange Commission released an interagency paper called "Sound Practices to Strengthen the Resilience of the U.S. Financial System" in which they addressed the need for major financial institutions and markets to provide adequate business continuity and disaster recovery plans to ensure the stability of the U.S. and world financial markets [U.S. Securities and Exchange Commission 2003]. However, as Mearian [2003] points out, some of the suggestions in the document are technically not feasible, including the notion that financial institutions have their primary and backup systems over 200 miles away because the native fiber channel technology used in storage area networks (SAN) has a limitation of 62 miles.

Organizations, managers, and IT specialists must realize that disaster recovery is a security concern. If someone breaks into an organization and steals the servers and destroys data, the organization is unable to function. A disaster that destroys equipment and data is no different; without these resources, organizations will not be able to function. Disaster recovery planning is also an issue for medium or even small organizations due to recent changes in legislation such as HIPPA (http://www.hipaa.org/). If the organization is responsible for the security of sensitive medical or financial data, the disaster recovery plan needs to consider the uninterrupted protection of that data. The Sarbanes-Oxley Act of 2002 also requires that organizations to maintain accurate and safe record keeping lest they be charged with negligence. In light of these issues, this article sets out to identify some of the key DR myths and offer best practices solutions for overcoming potential pitfalls. For courses on computer security to be truly effective, such issues must be covered as key components.

3. COMMON DISASTER RECOVERY MYTHS

3.1 Myth 1: The Only Disasters to Plan for are Natural Disasters

Every geographic region has its own unique threats – floods, tornadoes, tropical storms and hurricanes, fires, mudslides, earthquakes, blizzards, tsunami, and volcanic eruptions; every organization has something to plan for. The question is how are these disasters accounted for? Does the firm have the reserves to handle multiple disasters in a short period? While the likelihood of this is low, hurricanes Charley, Frances, Ivan, and Jeanne's visits to the Gulf coast states in August and September of 2004 and the 28 hurricanes and tropical storms of 2005 [NOAA 2007] are clear examples that multiple disaster do happen. For New Orleans, most of the problems caused by Hurricane Katrina happened after the storm. In addition to the tragic loss of life and property which was the direct result of storms, the long-term economic losses that could have been prevented with proper disaster recovery planning must also be considered.

3.1.1 *Power Issues.* As dramatically demonstrated by the 2001 power crisis in California and the August 2003 blackout in the northeastern United States, even with the ubiquitous nature of all infrastructure components, dependable power can be interrupted for long periods of time. The long-term economic impacts of the East coast blackout of 2003 have been widely debated, with estimates of direct economic costs ranging from the tens of millions in lost retail sales up to $6.4 billion for overall impact [Anderson and

Geckil 2003]. Back-up and alternate power supplies are no longer concerns for major manufacturing facilities and large-scale data centers only, but for small- and medium-sized businesses as well.

In 2004, the widespread impact of hurricanes Charley, Frances, and Ivan in August and September 2004 left thousands of businesses and households without power for three or more weeks. The long-term power outages were not limited to the areas of the hurricanes' landfall only, but extended well into Georgia and the Carolinas [Breed 2004; Brice and Langan 2004]. In New Orleans, Katrina left areas of the city without power for months. Due to power grids that were underground or had been submerged in salt water for three weeks, many organizations returning to their original homes had no electricity. Even three months after the storm, insufficient power and as little as one inch of rain compelled a key pumping station to go offline, and caused a key interstate, ironically a hurricane evacuation route, to be submerged in water for six hours. Many buildings lost power infrastructure, and had to rent semimounted power distribution equipment for months. After the storms in 2004 and 2005, there was a shortage of enterprise-scale power distribution equipment and qualified contractors to replace damaged electrical distribution equipment in high- rises in the central business districts.

3.1.2 *Environmental Issues*: *Heating, Cooling, and Humidity Control.* The emergence of clustered server environments in the late 1990s and early in the 21st century has marked a return to a more geographically centralized computing environment for many medium to large computing centers. In these massive multiprocessing settings heating, ventilation, and air-conditioning (HVAC) are key components. For many environments, electricity is backed up by a UPS for servers and network equipment, but not all UPS systems provide air conditioning. When server room temperatures exceeded acceptable operating ranges due to a power outage, some managers open doors and use fans to circulate air from outside into the server rooms. While the circulating air makes it feel better for people in the room, it has a devastating effect on the equipment, which now runs in an environment that is hotter and more humid than normal operating conditions, and now the air is unfiltered as well. The same water that damaged many electrical systems during Katrina damaged cooling systems as well, requiring many organizations to rent external chillers and park them outside their buildings to get HVAC operational. Many of the organizations in New Orleans that had back-up generators to cover electrical and HVAC needs had to shut down large water-cooled mainframe systems when city water pressure failed two days after the storm.

3.1.3 *Hardware Issues.* Every component in computers and computer networks will fail eventually, and as most IT professionals can attest, these failures usually occur at the worst possible times. If all of the back-up hardware is stored in the basement, even the equipment that survives the initial storm damage is prone to failure due to the hours spent in unacceptable environmental conditions. When fans, power supplies, and disk drives fail and there are either no spares, or worse all the spares are lost, are there contingency funds? Even if there are funds, there may be a severe shortage of some of the more common components. The ability to manage the payroll may be based on the ability to get the legacy parts you need from eBay. How will the purchasing department be convinced to place a bid on "Big Ed's Cool Stuff.com?" Many strategies have been developed to cope with these device failures, from the onsite service engineers with a room full of spare parts in mainframe shops, to guaranteed four-hour response times as part of service agreements with vendors, to clustered servers with fail-over capabilities.

The four-hour response deadline may not be met if vendors cannot get into the city due to road closures and mandatory evacuations.

Each strategy has its own set of advantages and disadvantages. The disadvantages can include difficulties like finding that proprietary blue widget with the special connector that was only produced for a few months back in the mid-1980s, to the overhead of warehousing spare parts for everything that might need replacement and paying the salaries of an in-house technical staff to do the repairs. On the plus side, a properly configured server cluster should be able to handle even multiple hardware failures without any noticeable impact to the end user. Onsite support staff with an inventory of spare parts can minimize the impact of hardware failures and drastically reduce recovery time since they are already familiar with all site-specific issues. Rapid-response service agreements with vendors may prove to be much more economical than having a firm's own onsite technical staff.

Due to the massive damage caused by Hurricane Katrina, there was limited access to many areas of metropolitan New Orleans. This meant that some companies could not get employees and supplies up and running for months. Even if employees could get back to certain areas with special passes, there was no place for them to stay, forcing them to commute for hours each way. For one municipal organization, there was no way to get a technical repair person in to the city to repair a remittance processing machine until the city opened up. The result was that the organization had several weeks worth of payments in checks with no way to process them.

3.1.4 Software Issues. What would happen in most businesses if an operating system, office-suite product update, or service pack produced some crippling software conflict? Software problems can range from interoperability problems to license issues. Almost immediately after Microsoft Office 2000 was released, many IT support centers and help desks were besieged with calls from frustrated users complaining that whenever they tried to open an office application they would experience the dreaded "blue screen of death." More recently, the release of Microsoft Windows XP service pack 2 (SP2) had crippled many users despite the well-publicized software and hardware conflicts and the efforts of many IT shops to warn users about site-specific conflicts. With proper planning, back-out from implementations of new hardware or software can be accomplished, but without contingency plans the disruptions to regular business activities can be catastrophic. Due to the varied nature of end- user PCs and environments, it should never be assumed that just because software installations and upgrades worked in one environment, they will work in all versions. Even among standardized environments such as the U.S. Navy's implementation of the Navy Marine Corps Intranet (NMCI), there are different versions and hence compatibility issues.

3.1.5 *Virus and Worms.* As shown by outbreaks like the Melissa virus and worms like Slammer, Blaster, SoBig, and MyDoom, the new viruses and worms can propagate and spread at alarming speeds. Even when the software producers release patches, many vulnerabilities remain in systems that are not properly maintained. One glaring example is the Slammer outbreak that targeted unpatched Microsoft SQL servers. Even though the patch had been publicly available for a full six months, literally thousands of systems were affected. Unsecured and improperly maintained systems are part of a growing problem as more powerful computers and broadband Internet connections become more prevalent. Increasingly, a colleague's system security is as much an issue as the security of one's own systems. As a result, all equipment must be patched and audited. If it is not possible to audit all systems via automated tools, then at a minimum random sampling must be used to ensure that patches are actually being deployed, and deployed correctly.

3.2 MYTH 2: A Mock Test Really Tests Disaster Recovery

Any plan that has never been fully tested is useless: for example, the air-traffic control radio failure in Los Angeles in September 2004. When a routine monthly maintenance check was missed, the radio system shut down. The back-up system did not work because it "was not configured properly to ensure its availability in the event of the primary system's failure" [Blood 2004].

Quite often, organizations choose to perform a mock DR test. The process is simple: employees are warned weeks before the event; the disaster is simulated, and employees restore key systems on back-up hardware and facilities. But just as in the case of the air-traffic control radio, how does an organization know that the DR system will really work when it counts? Key items such as telephone numbers and Internet addresses are not fully tested. In a real disaster the consequence of not testing these items means that customers have no way to contact the firm and conduct transactions. Firms must ask whether or not a test under optimal conditions really proves the validity of the DR plan. If all key personnel are standing by with everything they need to complete all of the tasks outlined in the planned test, did they really test anything other than the organization's ability to plan a test? What does the firm do when 75 percent of the staff is missing? Are the processes documented so that the survivors can pick up the pieces and continue operations? Often, it is the simple questions that are overlooked: for example, how will mission- critical staff communicate in the absence of e-mail servers, cellular phones, or traditional telephone systems? The first step in ensuring that mission-critical staff can communicate in an emergency is to test the DR plan by bringing components down to ensure that the plan really works. According to Jeffrey Schilit, associate provost and CIO at Florida Atlantic University, the reason for not conducting a real DR simulation is the lack of "time, energy, resources." According to Schilit, it takes four hours to shut down all of the university systems and another four hours to restore them [Foster 2004]. For a university that is on the Florida coastline and likely to be severely impacted by hurricanes, this is a very dangerous position to take.

For a DR test to be useful, an organization must ensure that the test really does test what it is supposed to test. Without real testing, there is no proof that the plan actually works. The firm should have detailed logs of what works and what does not. The "lessons learned" must be noted and applied post-test, and anything that did not work every time must be addressed immediately. One of the lessons learned from Katrina is not to put all of your eggs in any one communications basket. Key staff needs to share "non-work" e-mail addresses and the out-of-state contact information of their friends and family, as well as a contact of last resort. Almost everyone will contact their families as soon as they can and leave messages with family members. After Katrina, many employees did not know whether they still had jobs; in a chaotic situation a means to contact employees to tell them that they have jobs and how they can do them is very important.

The consequence of a mock DR test is the assumption that other key systems will remain available. The reality, confirmed by Katrina, is that key systems were unavailable, and could not transition back to their original condition in a few days, as expected. Many systems did not transition to their original condition until many months later. For organizations that planned to work manually for a few days only, the reality was that they could not do so for months.

3.3 Myth 3: Attacks and Hacks Are Only External Threats

It is important to remember that employees can be a source of intentional or unintentional attacks on corporate resources. Internal attacks are much more devastating than external ones due to faster connectivity on local intranets and the fact that most organizations feel they can trust employee workstations. Viruses and worms are not only threats to e-mail and PCs, the So-Big and Blaster worms and variants show that they can devastate networks and networked applications as well. In terms of best practices, employees should realize that attacks can come from anywhere. To prevent this, there should be clear procedures in place to remove a PC, network, or building from the enterprise network in order to ensure that key business functions take place within the enterprise.

3.3.1 *External Attacks.* Owing to the Web, internationally known companies such as Amazon.com, eBay, and Yahoo have been the victims of distributed denial of service (DDoS) attacks. Such attacks are intended to disrupt the victim's business by "clogging its Internet pipe" with spurious traffic. The usual attack strategy is to compromise as many unsecured client computers on as many Internet-connected networks as possible and deposit small programs on them. At a predetermined time, all of the "zombies" or "bots" will participate in a DDoS attack on a prearranged target. These attacks usually take place without the owners of the compromised systems being aware that their computers and networks have been harnessed for such activities.

Following a disturbing trend, DDoS attacks are becoming part of more sophisticated virus and worm attacks. As in the case of the MyDoom outbreak of early 2004, infected computers were not only used to spread the malicious code, but were also harnessed to attack common sources of software patches and updates for commercially available antivirus software. This limited the ability of the legitimate computing community to respond to the outbreak. Landry et al. [2006] outline that all systems should be firewalled for both academic and corporate environments. In an effort to get systems up quickly after Katrina, many organizations brought systems online and connected to the Internet without firewalls and other security measures. The mandate from management was to get the systems up quickly, and protect them later. The truth is that these systems should have been protected as soon as they went online; firewall and other security measures must be part of the solution. Security cannot be an afterthought.

Not all external attacks are cyber-attacks. Many of the most successful hackers have used "social engineering" to penetrate an organization's network and computer security. With a little knowledge of an organization's structure and a few publicly available names, a bold con artist can bluff his or her way into most offices. In our society, people are generally trusting, and as a result they can easily fall victim to social engineering. How many new hires or temporary staffers wouldn't fall for "Hi, I'm Bob from the Help Desk – Mr. Jones asked that we take his computer back to the IT shop right away so that we can perform an upgrade while he's out of the office."

In the hurry to get systems up, it is not known how many companies fall victim to social engineering attacks. People and organizations prey on victims with quick-fix scams. In post Hurricane Katrina New Orleans, how many systems containing sensitive data were stolen by looters? How many of the looted pharmacies used encrypted file systems? How many computers were hauled off to landfills before being "scrubbed"? This sensitive data when recovered from discarded hard drives and other secondary storage mediums provide the perfect launching pad for myriad external attacks.

3.3.2 *Internal Attacks.* It has always been the case that disaffected employees pose the greatest threat to an organization. As computer and network access become more ubiquitous in the workplace, there are more chances for abuse. With an insider's access and knowledge, trusted employees can cause as much if not more harm than any external threat. If there is reason to suspect that an employee may intentionally compromise electronically stored information, or the systems used to store and process it, then the only reasonable response is to remove that employee's access to it. The 2004 theft of 92 million AOL screen names and credit card information by an AOL employee is a clear example that internal attacks and inappropriate data access can be a disaster [Krim and Vise 2004]. Similar to external security devices, internal devices need to be present as well. During a disaster, there is enough confusion and lack of audit trails in an organization for employees to potentially take advantage of the situation.

3.4 Myth 4: Untested Disaster Recovery Hot Sites

In many organizations there is the prevailing notion that in the event of a disaster, employees will conduct business at the DR site. The problem is that many employees have never set foot in it, and to search for the DR site in an emergency is one of the worst things that can happen. All key DR employees should be very familiar with the DR site, since this is no time to learn a new environment. Nor is a crisis, with its accompanying heavy vehicular traffic, the time to start looking for a new location. Drivers who evacuated New Orleans for hurricane Ivan in September 2004 found that a drive that normally took one hour took between five to eight hours. On the positive side, by staggering the Katrina evacuation and reversing traffic flow, over 2 million coastal residents were evacuated successfully, a direct result of the lessons learned from Ivan the year before. However, Hurricane Rita in September 2005 left drivers in the Houston area on the road for over 24 hours demonstrating that there is no good way to move 3 or 4 million people all at once.

Additionally, there may not be sufficient power, cooling, network, phone, and space resources available. There must be enough keyboards, monitors, power strips, network cables, and so on, for people to work. Going to a local computer supplier during an emergency may not be an option. If the site has never really been tested, there is no way to count on the site working. Also consider the following: Will the employees have all the data they need on a regular basis? Will the local Internet service provider be able to get adequate service in a timely manner? Organizations in the post-Katrina environment ran off residential broadband connections for months, which took weeks to get set up. The assumption may be that all files are stored on the server, but users may rely on local PC data and applications. Worse yet, they may not know where the data actually resides, and once the employees are on site the problem will be to reroute customers and business functions to the hot site. The only way to make sure that there are sufficient power, cooling, network, phone, and space resources is to regularly test the site and to reroute customers to ensure failover (the transfer of data and processing power from a failed system to another) can occur during a nonpeak time. Alternate accounts payable / receivable procedures must also be part of the plan; if payments cannot be collected for three months there will certainly be trouble.

For server rooms, it will be necessary to acquire more space and more server consoles than normal. During a disaster it is quite common that every server will need to be shut down and be restarted later, and that system administrators will need to access every server console. While it is unlikely during normal business operations, the need to share monitor, mouse, and keyboard systems for dozens of servers will result in server administrators lining up to get to their resources. This bottleneck translates directly into longer downtimes. Remember, remote access to server resources may not initially be available, so direct physical access to servers may be required.

3.5 Myth 5: Conference Rooms Are Adequate Disaster Recovery Sites

Due to limited resources, not all organizations can have two sites where all employees can work in the event of a disaster. So setting up alternative sites, which normally serve a different purpose, to house employees during a disaster seems a good idea. However many organizations select rooms that are generally unsuitable as working spaces, for example, a conference room. Conference rooms are not offices, and are not equipped like offices. Generally speaking, such areas are not equipped to handle users' numerous telephone lines, power, and networking needs. There is also the issue of simple things like office supplies; emergency sites should be stocked with basic office supplies, which will be needed by the transient workforce. Another potential problem is that more than one department may decide to relocate to the conference room. Allocation of physical space and vital resources (e.g., number of available phone lines and network connections) needs to be addressed by the disaster recovery plan. In larger organizations, the allocation of resources in the event of a disaster may require arbitration between the various stakeholders, but these issues should be resolved in advance as part of an effective disaster recovery plan.

It is also important to make sure that there are enough wired telephone lines, as cellular service may be saturated or unavailable during a disaster. The organization should not rely on any resource that is not under their direct control. Cellular phone networks, power grids, and Internet access are usually provided by external vendors who may or may not be able to meet the organization's needs in a post-disaster environment. The vendors on whom businesses rely should have their own DR plans and these plans should be shared. Katrina demonstrated that using a conference room at another facility is not enough. In reality, people worked everywhere, including on floors and in hallways, and some with the possibility of having no place to live for an extended period. In addition to workspace, the problem of housing employees for an extended period of time must be dealt with: two to three months of hotel bills for hundreds or thousands of employees can be incredibly expensive. There needs to be a plan for corporate housing should the disaster not be a seven-day event. And if the organization is going to provide temporary housing such as trailers, where will they be located and when should the decisions be made?

3.6 Myth 6: Disaster Recovery Can Be Implemented Later

To reduce development time and costs, DR is, quite often, an afterthought or is planned for a later date. The problem is that often planning and budgeting do not happen at a later date. The reasons are simple: once systems are put into production, it is difficult to find the time and the means to implement and test a DR plan; additional overtime costs will be incurred for after-hours testing once the project is complete; it may be difficult to acquire the resources at a later date; and instituting DR plans later means the system will have to be tested with downtime. In today's global 24/7 world, this is very unrealistic. The only way to ensure that a DR plan will work is to ensure that DR planning and testing occur prior to implementation for every installation, upgrade, and new project. Anything less means that the system has not really been tested. The claim that DR testing will be done later is false, most often it will not. As a result, organizations develop the mantra: "If the current system fails, we can use the old system instead." There are a number of problems with this solution. First, the data on the old system may not be current and the application may not be installed or compatible with the other systems in place for all clients. Does the organization still have all the required technology for the old system? Is the old technology even available? Furthermore, the current users may not know the old application and the old system may not meet current business and legal requirements. Lastly, in the case of a physical disaster, the old system may also be compromised. There are very few organizations that can truthfully say that they can use their old systems. A few, such as Care Group, were able to use their old paper systems because they made sure that the systems were available as a Y2K contingency [McFarlan and Austin 2003]. But the farther away from Y2K, the more unlikely an alternative this will become. Again, this plan was proved flawed in the post-Katrina environment, when organizations that planned to run manually for a few days realized they could not continue to do so for months.

This approach works only if the old systems still match the needs of the business functions and if the data is maintained. An older server may not be able to be reactivated and run the current applications. Quite often new servers have more capacity than the previous hardware, and there is not enough capacity to revert. If a new version of an application differs from an old one, the old application must be maintained on the workstations and servers. In terms of best practices, business users should consider the following: use similar hardware as a secondary source to roll back to and make sure that it is used and tested regularly; ensure that hardware and software receive regular product updates and service packs; ensure that hardware and software are covered under maintenance; and use secondary hardware as a staging ground for testing new releases and configurations.

3.7 Myth 7: Equipment Will Be Available During and After the Disaster

A plan that will not work is the notion of moving key equipment during a disaster. Loss of power means no elevators, and in the event of a physical disaster, there may not be anything to move. For an impending event such as a natural disaster (hurricane, flooding, etc.) that has been forecasted, business owners must decide when to shut down production systems prior to the disaster in order to do back-ups and start to move equipment. When people in New Orleans went home on Friday, Katrina was a storm that was going to hit Florida – by Sunday it was the Apocalypse for New Orleans. People were caught unawares; by the time they knew the storm was coming it was too late to return to New Orleans and take protective measures; and they had to ensure the safety of their homes and families first. Employees who stayed behind in downtown New Orleans found themselves being rescued by rubber rafts and helicopters. Staff that is responsible for protecting key systems and equipment needs adequate time to ensure their own safety after the relocation of equipment has been completed. The solution is to test and prove redundant or secondary equipment off site. No exceptions.

Similarly, buying a new server during or right after DR is not feasible. Organizations must know how much time it will take to order and receive servers and network equipment, taking into account that other organizations are trying to order the same equipment at the same time and thus causing shortages. Four months after Katrina, many areas of Louisiana were still not getting regular service from the U.S. Postal Service. Next day air shipments were taking up to four business days even months later. It also assumes that purchasing systems will work in a DR scenario. Once the servers arrive, organizations need to determine how long it will take to install the servers, networks, and applications. Finally, they should determine how many resources it will take to set-up and rebuild all applications, networks, and servers all at once. Alternatively, contracting for replacement equipment with providers of DR solutions is possible. Firms must also ensure that providers of DR solutions are notified whenever systems are upgraded or changed.

3.8 Myth 8: Back-Ups Work

Unfortunately, having a stack of back-up tapes does not necessarily mean that the data can be successfully restored. So the first thing to identify is the back-up strategy. Is it consistent across systems, or do individual departments have different strategies? Once a strategy has been determined, when was the system tested? Was a restore done on the same server or on new equipment? Both scenarios must be tested. The next concern is the length of time it will take to restore the system. Furthermore, databases and other files that are routinely open may not be backed-up. Even if the back-up software has an open file agent, there is a good chance that databases will not be restored successfully. In the case of a physical disaster, there may not be a current or legacy system to restore to.

Firms should mandate that all servers have a rigorous testing plan for back-ups before going into production. This means the data is backed up to tape, drives erased, and all data restored, not just a few files; a new "fresh-out-of-the-box" server will be useless if the data cannot be restored. Test back-ups on a regular basis to ensure that tapes actually contain data; work with database administrators to ensure that databases and other open file systems are being backed up and can be restored correctly; and have a benchmark for how long a tape restore should take. A further requirement is that back-up tuning is in place to reduce restoration times. And, potentially, what happens when the production server and the DR server are both on the corporate intranet with the same server name and DNS entries. Many organizations post-Katrina had problems when they restored their production servers and, due to naming conflicts, could not copy data over. Worse yet, IP address conflicts could route employees and customers to the incorrect server with stale data or data that would be overwritten and lost. Such potential problems have to be tested for and dealt with before a disaster occurs. Furthermore, what happens to the information stored on back-up tapes? Information stored on servers is secured by file permissions, user IDs, and firewalls, but once the data is on tape, where is the storage area and who has access to it? In December 2005, Marriott Vacation Club International announced that back-ups containing credit card data and addresses for customers and employees was lost in mid-November [Reuters 2005].

3.9 Myth 9: Disaster Recovery Can be Planned Individually

Planning for disaster recovery must be centrally coordinated, and the larger and more complex the organization, the more important this becomes. There needs to be a centralized process for all DR plans, so that individual departments or other units aren't replicating the same processes (e.g., not everyone can use the conference room as an alternate office space). The conference room or other DR area may be confiscated by state and federal agencies, the National Guard, or FEMA. If this happens, what is the next planned step? Carefully thought out contingency plans must include the possibility that the desired site may not be available. Each organizational unit needs to know where and how they fit the DR plan. Hand-offs between departments and working groups must also be planned for. Simple issues such as how time-sheets will be handled need attention, as well as larger ones like how suppliers can contact the business to schedule deliveries during a disaster-recovery effort. A DR officer must coordinate recovery plans with employees, departments, partners, and vendors. There must be a coordinated effort among departments and applications. DR plans should be given to contractors and vendors as well, as their help will be needed in a true emergency. The DR plan should be simple and available. A clear chain of command accountable for giving clear directions during a confusing time is a necessity.

3.10 Myth 10: Everyone Knows What to Do

Staff roles should be clearly identified and communicated before a disaster. Lines of authority and succession should be established before an emergency as part of the DR plan: not everyone may survive and all survivors may not return. In a natural disaster, local officials may suggest a voluntary evacuation or order a mandatory one. The decision to shift operations to an alternate site needs to leave enough time for people to provide for the safety of their families and property before they report to an alternate site. Ideally, the alternate site should be activated before the primary one is shut down. Before employees leave, arrangements must be made to ensure there are adequate hotel rooms for employees and their families. However, not everyone needs to be at the DR site. Who goes and who stays? When should they leave? Where will they go? These are all questions that have to be determined ahead of time. Lack of valid information during a disaster only makes things worse. Finding out that key employees are riding out a hurricane in 8 to 12 feet of water is not only very distressing, but leads to confusion and chaos. In the event that a key manager or employee is unavailable, a clear chain of command must be established so that all employees know who the next person in charge will be.

Key roles and teams must be defined ahead of time, including identifying those who play key roles in each application. Who will be responsible for each aspect of the business at the alternate site? Will there be a transitional team while the regular employees make their way to an alternate site? Who can fill in when a key employee cannot be found? There must be a clearly defined line of progression for each key role. Every key employee must have at least one back-up, and that backup needs to receive regular cross-training. In the event of a disaster, not everyone may be able to report to an alternate site.

Many key employees could be in evacuation shelters and not be allowed to leave to until the crisis is over. So for routine functions, there should be plans to leverage vendors and contractors in times of crisis. Many tasks other than the core competencies of the organization could be outsourced during a period of disaster recovery: with proper testing, janitorial staffing, physical security, onsite IT support, and even simple payroll functions could all be reasonable candidates for temporary outsourcing. At the University of New Orleans, a decision was made after the hurricane to outsource Blackboard content management services directly to Blackboard.com after server resources at the university became unreachable. Unfortunately, because this decision was made after the storm and not as part of a DR plan, class roles, content, and user accounts had to be created from scratch during a chaotic time. Had it been part of a DR plan, data and user accounts could have been pre-staged before the disaster.

Whenever possible, some staff needs to be at the DR site ahead of a natural disaster. Some people need to stay at the main site with remote connectivity to both sites to ensure a smooth transition. Developing relationships with vendors and contractors ahead of time will make this process smoother. This means securing contracts ahead of time so that vendors and contractors can work at a given organization; it may also involve background checks on the vendors and contractors. To enable employees, vendors, and contractors to pitch in, connectivity to main and remote sites must be tested during business and off-hours, and key documents must be made available to them. If all configurations and key documents are stored only on the servers, the documents needed to restore a given server will be unreachable. To avoid this catch-22 scenario, all detailed documents as well as contracts and service numbers must be stored off-site. Finally, key employees should have key documents at home, with instructions that during a DR those documents be on their persons.

Another concern is contacting employees. Traditional phone lines and cellular equipment may be damaged or simply overloaded. These temporary outages are routine during disasters, during peak-traffic times, major sporting events, and conferences. Disaster recovery plans should include alternate means of communication in case the publicly available communications infrastructure fails. During and after Katrina, cellular telephones did not work, and when they did, calls were frequently dropped. Surprisingly, text messaging did work; but many people did not know how to text message or their phones did not have that capability. Everyone needs to have plans for accessing the Internet from wherever they are and using alternate e-mail providers such as yahoo, hotmail, gmail, and so on. National services should be used, and not those that are local or ISP-based, as they may be knocked out by the same event that took out local e-mail servers. Employees should have basic web skills, and even the most senior management should get to web enabled e-mail.

4. SUMMARY

Technology will not save an organization from a disaster. There are no “silver bullet” fixes. Organizations should consider every possible threat no matter how unlikely and unthinkable it is. Flexibility and a clear understanding of the core objectives are crucial. Understanding that task A must be accomplished rather than obsessing over how to recreate every aspect of the “regular” environment is often more effective in time and cost. Organizations that take a pessimistic approach to disaster recovery will be better prepared than those that do not. An examination of recent history shows that very unlikely events can and do occur: statewide power outages (August 2003); disappearing buildings and resources (September 11, 2001); redundant hardware failures (September 2004); the number and frequency of storms (2004 and 2005), and other formerly unthinkable scenarios show that disasters do occur. Hurricane Katrina was one of the worst disasters in American history; however many lessons were learned from it and other disasters.

The solution is simple. Developing comprehensive plans that have been tested and can be implemented is the only thing that can save an organization. Successful DR plans must have top-down management support. However, a DR plan that has been devised and tested is not good forever. Business processes and technology change frequently in today’s environment, and DR must change accordingly. DR planning is an ongoing task, not a one-time goal, so capital budgets must include items for maintaining DR sites and equipment. If these concepts are integrated into network security classes, students will be better prepared for real-world IT experiences.

REFERENCES

ANDERSON, P.L. AND GECKIL, I. K. 2003. Northeast blackout likely to reduce US earnings by $6.4 billion. http://www.andersoneconomicgroup.com/modules.php?name=Content&pa=disp_file&doc_id=544

BLOOD, M.R. 2004. FAA blames maintenance glitch for loss of radio link with pilots. *Houston Chronicle* (Sept.16), A5.

BREED, A.G. 2004. Frances leaves floods, power outages, takes aim at panhandle. *Billings Gazette* (Sept. 6). http://www.billingsgazette.com/index.php?id=1&display=rednews/2004/09/06/build/nation/30-hurricane-frances.inc

BRICE, J. AND LANGAN, H. 2004. Ivan leaves about 1.6 mln without power in U.S. south. *Bloomberg* (Sept.17). http://quote.bloomberg.com/apps/news?pid=10000103&sid=azVDltxOaqms&refer=us

FOSTER, A.L. 2004. Insecure and unaware. *The Chronicle of Higher Education* (May 7), A33-A35.

KRIM, J. AND VISE, D.A. 2004. AOL employee charged in theft of screen names. *Washington Post* (June 24), A01. http://www.washingtonpost.com/wp-dyn/articles/A860-2004Jun23.html

LANDRY, B.J.L., MAHESH, S., AND KOGER, M.S. 2006. Firewall strategies for protecting academic resources and teaching network security. In *Proceedings of the Southwest Decision Sciences International* (Dallas, TX).

MCFARLAN, F.W. AND AUSTIN, R.D. 2003. CareGroup. *Harvard Business Review*.

MEARIAN, L. 2003. U.S. regulators issue disaster recovery guidelines. *Computerworld* (April 11). http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,80262,00.html

NOAA. 2006. 2005 Atlantic hurricane season. http://www.nhc.noaa.gov/2005atlan.shtml

REUTERS 2005. Marriott vacation club reports missing data tapes – Contained information on 206,000 customers, employees. Dec. 28, 2005. http://www.computerworld.com/securitytopics/security/story/0,10801,107366,00.html?source=NLT_DIS&nid=107366

U.S. SECURITIES AND EXCHANGE COMMISSION. 2003. Interagency paper on sound practices to strengthen the resilience of the U.S. financial system. http://www.sec.gov/news/studies/34-47638.htm

Received January 2006; revised June 2006; accepted June 2006