RECOVERING IT IN A DISASTER: LESSONS FROM HURRICANE KATRINA

Executive Summary

On August 29, 2005, Hurricane Katrina destroyed a data center and much of the communications infrastructure at the Pascagoula and Gulfport, Mississippi, operations of the Ship Systems sector of Northrop Grumman Corporation. Simultaneously, the hurricane put a second data center out of commission in a shipyard near New Orleans. The storm disrupted the lives of the sector’s 20,000 employees and their dependents located in the Gulf Coast, caused over US$1 billion in damage for the company, and, for two weeks, brought two of the nation’s largest shipyards to a standstill.

Northrop Grumman’s experience provides a rich opportunity to look at the consequences of, and responses to, a cataclysmic disaster—one that, by its magnitude, far exceeded the assumptions of most firms’ business continuity plans. This story of resilience, agility, and recovery provides valuable lessons in how to adapt when the business continuity plan and when the public infrastructure prove inadequate. This story also provides an opportunity to reexamine our processes for preparing disaster plans, as well as processes for assessing preparedness and response after a disaster or a near-disaster.

THE REALITY OF DISASTER PREPAREDNESS

“Two days after Katrina smashed into two of our data centers in the Gulf Coast, one of our guys rushed into our recovery center carrying large binders. ‘Thank God,’ he announced, dropping the heavy load on a conference table, ‘we’ve recovered the IT disaster recovery plan for the Ship Systems sector.’ My immediate response was, ‘I’ll be glad when we can do our disaster recovery plan. ’Right then, we weren’t doing any of that. We were doing what the company needed us to do.”

Tom Shelman
Vice President and Chief Information Officer
Northrop Grumman Corporation

Tornadoes, fires, hurricanes, earthquakes, collapsed dams or broken water mains are worst-case scenarios for CIOs. Potentially massive disruptions in information technology can cripple, even destroy, a business. Today, the list of threats must also include bombs, cyber terrorism, and fast-moving viruses in humans. As the avian influenza illustrated, when viruses mutate to a form easily spread among humans, they can spread worldwide in a matter of weeks, perhaps kill millions, and curtail business and constrain social life for months. For large, widely distributed firms, these threats

1 Jeanne Ross was the accepting Senior Editor for this article.
are real. In a recent study commissioned by AT&T, 30 percent of the responding senior IT executives reported that their company had suffered from some form of disaster in recent years.\(^4\)

Planning for disasters and recovery is essential. But the threats come in many forms, forcing planners to make assumptions about the probability, nature, and magnitude of the potential threats. What happens when these assumptions prove to underestimate a business continuity disruption? This article explores the experiences of Northrop Grumman Corporation, whose Gulf Coast facilities, employees, and communications and information infrastructure fell directly in the path of Hurricane Katrina. As CIO Tom Shelman’s earlier quote illustrates, Northrop Grumman Corporation had a business continuity plan, but Katrina far exceeded some of the plan’s underlying assumptions. Shelman and his organization, therefore, had to operate outside the bounds of that plan. This article describes their efforts and presents current thinking about disaster preparedness.\(^5\)

THE SHIP SYSTEMS SECTOR: IN THE PATH OF DESTRUCTION

Early on the morning of August 29, 2005, Hurricane Katrina made landfall near the Mississippi-Louisiana border. It battered the Mississippi coast with a storm surge reaching 30 feet in height in some locations and with hurricane-force winds extending 200 miles inland. In Mississippi, Katrina was responsible for 239 deaths and the destruction of some 65,000 homes.\(^6\) New Orleans was spared the surge and much of the wind, but in the hours after the storm, the city’s levees gave way. The resulting flood devastated much of the city and neighboring parishes. Despite a mass evacuation and thousands of rooftop rescues, 1,100 people in and around New Orleans lost their lives.

The long-term implications are still dire, particularly in New Orleans. Over 780,000 people were displaced, many permanently. More than 200,000 homes suffered major damage and 250,000 people were at least temporarily put out of work. The population of New Orleans was, and remains, dramatically lower, while Baton Rouge, Houston, Atlanta, and Dallas experienced large influxes of evacuees.

Northrop Grumman Corporation

Northrop Grumman Corporation is a US$30 billion global defense and technology company whose 122,000 employees provide innovative systems, products, and solutions in information and services, electronics, aerospace, and shipbuilding to government and commercial customers worldwide. Ship construction is a major business, accounting for revenues of US$5.7 billion in 2005. In August 2005, Northrop Grumman’s Ship Systems sector built large military vessels, primarily for the U.S. Department of Defense and the Navy.

Approximately 20,000 Ship Systems employees worked out of three large facilities in the Gulf. A facility in Pascagoula, Mississippi, together with a smaller shipyard in neighboring Gulfport, employed approximately 12,900 workers. Most of the other 7,100 employees worked at the New Orleans yard, located in Jefferson Parish, Louisiana, near New Orleans, approximately 124 miles west of Pascagoula.

Preparing for a Hurricane

Hurricane preparation was nothing new to the Ship Systems sector, its CIO Jan Rideout, or its 200 IT professionals located at its Gulf Coast facilities. In September 2004, Hurricane Ivan had threatened these facilities, so Rideout’s team had carefully secured its IT assets. Ten months later, in July 2005, when Hurricane Dennis threatened, they did the same. Fortunately, both storms missed the sector’s facilities. The following month, though, luck ran out. On August 26, 2005, a commercial weather forecaster advised Northrop Grumman management that another powerful hurricane, Katrina, was bearing down on the Gulf Coast. Katrina had already left 11 people dead and over US$1 billion in damage in Florida. It was headed for a predicted landfall in Louisiana or Mississippi.

Rideout’s team took the usual precautions. Data backups were sent to Iron Mountain, as well as to Northrop Grumman’s Dallas location. Most servers were powered off and wrapped in plastic. A newly installed backup generator, located in a relatively secure location, allowed them to leave some essential servers running. Several hours before evacuation, these servers were switched over to the auxiliary generators. Just one application was kept live: an extranet that


\(^5\) Northrop Grumman Corporation’s experience recovering from Hurricane Katrina is also documented in a case study suitable for use in educational programs: Ives, B. and Junglas, I. “Information Systems in Hurricane Katrina Recovery”, in Communications of the AIS, Volume 18, Article 27, 2006.

supported development of a new class of destroyers, the DDG 1000. 7 This system was a crucial resource for Northrop Grumman, the Navy, the Department of Defense, and other suppliers. It was particularly crucial at the time because a critical design review was just two weeks away.

With the preparations complete in both Pascagoula and New Orleans, and facing a mandatory evacuation order, Rideout and her team left the area. Some headed east; Rideout ended up in a small hotel room in Georgia with her husband and dogs. Others headed to Mississippi, northern Louisiana, or settled in with friends or into motels further inland. Rideout’s team, like tens of thousands of other Ship Systems employees and their family members, soon was widely scattered, but generally out of harm’s way.

THE FURY OF KATRINA

The storm smashed ashore the morning of August 29, a Monday. In Dallas, Shelman and his management team closely monitored the storm’s relentless march across the Gulf of Mexico. By Monday night, it was apparent from news reports that both the Ship Sector’s Pascagoula and New Orleans facilities had been in the storm’s path. Throughout the day, Shelman’s management team had been unable to reach any of their people in the area.

Early Tuesday morning, the first report came in to Philip Teel, president of Northrop Grumman’s Ship Systems sector; the news from the Pascagoula yard’s storm ride-out team was bad. At 6:30 a.m., Shelman learned that there had been some damage to several ships under construction and extensive damage to the shipyard and nearby communities. The shipbuilding business, as well as the lives and well-being of the Ship Systems sector’s 20,000 employees and their approximately 60,000 dependents were at risk. Grabbing his cell phone, Shelman began his 90-minute commute to work. In the car, he began to pull together the first stages of the Northrop Grumman disaster recovery response.

By the time he reached his Dallas office, his conference room had been transformed into an emergency command center. Computers, phones, and a local area network were already in place; the newly assembled members of the command center were already struggling to reach employees in the impacted area. Other managers were told to stay available for assignment.

Information dribbled in. Several employees living adjacent to the areas affected by the storm were reachable by phone, e-mail, or text messages. Some evacuees, including Sector CIO Rideout, began to call in. But information about damage in the storm-struck facilities was, at best, sketchy.

Later Tuesday morning, they learned that Trent Lott Field, a regional airport near the Pascagoula yard, was open, though only for daylight takeoffs and landings. There was a small window to get someone in and out that day. Morales, a Colonel in the Army Reserves who had served in both Gulf conflicts, volunteered to take a camera and fly in on a corporate jet.

Extensive Damage in the Pascagoula and Gulfport Yards

The digital images sent back the following day to Dallas, as well as Morales’s verbal reports via satellite phone, painted a dismaying picture of massive devastation. Most notable were the giant casino barges that had washed off their moorings and floated ashore. They blocked the highway and crushed buildings. Hotels and casinos were badly damaged, some beyond repair. Restaurants, businesses, and miles of beachfront houses had been washed away or severely damaged.

Rideout learned that her own beachfront house was gone, washed off its piers into the Gulf of Mexico. Many of her employees had lost their homes or returned to find them extensively damaged. Several recounted harrowing escapes from the storm; others, including two of Rideout’s neighbors, had ignored the evacuation orders and died from the massive storm surge. For many of those who chose to return, the agony was just beginning. With the housing stock severely disrupted, many employees and their families would move in with friends or relatives. Others lived for months in motel rooms or recreational vehicles or faced long commutes from communities spared by the storm.

Fortunately, damage to the ships in the yard was, with one exception, relatively light; the large cranes and fabrication facilities had also generally survived, but with extensive damage. Anything with an electrical motor exposed to the corrosion of salt water was destroyed or required extensive repair. Among these were lathes, drill presses, and other electrical equipment, as well as some of the more modern cranes. Construction materials, including miles of metal piping, were scattered everywhere. A major loss was the scores of small frame buildings previously located throughout the yard. These semi-portable

---

7 DDG 1000 is the next generation Navy destroyer.
buildings housed the engineers and managers watching over particular phases of construction. As construction proceeded and the ships moved, the buildings were moved as well. Now, those buildings, and the desks, files, computers, phones, walkie-talkies, and blueprints that had been sheltered within them, were floating in the Gulf of Mexico or scattered about the yard.

The news regarding the IT infrastructure was bad. A subsequent study revealed that 1,500 personal computers had been lost, as well as 200 servers, 300 printers, 600 data input devices, and hundreds of two-way radios. The surge had destroyed the yard’s primary data center, including servers and communications gear. Other core communications equipment that had been located in a more elevated location had escaped damage; but most of the network infrastructure in the 675-acre yard was gone: communications closets, routers, switches, as well as fiber and copper cables and wires. In addition to the loss of the local and metropolitan network connectivity, the wide area network that linked Pascagoula to the rest of the sector and the company no longer worked.

**Damage at the New Orleans Yard**

The Ship Systems sector’s New Orleans yard had also been affected by the storm. The day of the storm, the Dallas team had gotten a message through a BlackBerry of an employee who worked at the yard but lived 50 miles west. The following day, that employee, Lonnie Frazier, was tasked with trying to reach the plant; two days later, he succeeded. He reported that the New Orleans yard, located to the west of the full force of the hurricane, was not too badly damaged nor had it been physically damaged by the flooding after the levees surrounding New Orleans were breached.

The IT damage reports were far more encouraging for the New Orleans yard than for the Mississippi facilities. Much of the communications infrastructure had survived the storm in New Orleans, as had servers and desktops. Several servers continued to operate throughout the storm, including those supporting e-mail and instant messaging. But a subsequent failure in the air conditioning system led to an automatic shutdown of the servers and their communications. For about a week after the storm, some phone lines were still useable, though only for incoming calls; a T3 communications link to the outside world still operated. A week after the storm, communications suddenly failed, reportedly due to communications lines that had been downed by the storm and eventually severed by cars repeatedly driving over them as they drove into or out of the yard.

Failures in the public infrastructure, combined with security concerns, disrupted the New Orleans yard for weeks. For many days, access to the parish in which the yard was located was tightly controlled and limited to daylight hours. It became apparent to the team in Dallas that neither Gulf Coast data center would be available anytime soon. The Pascagoula center might never be available.

**GETTING PEOPLE BACK TO WORK**

The Northrop Grumman disaster recovery team soon realized that its biggest challenge differed significantly from what it had expected the day before the storm. Shelman explained:

“First, you think this is about restoring computer systems, but it’s actually about putting our employees’ lives back in order. I now understood our mission was not about recovering data centers or computers, it was about 80,000 lives. That was our mission, and I reminded people about it several times a day.”

The crisis team immediately recognized that the early stages of recovery were far more about restoring human resources than restoring information systems; nothing could be done without personnel. Nor could the shipyards get back in operation without personnel. But sector personnel had become widely scattered about the Gulf Coast and neighboring states, and they were focused on the safety of their families, friends, and homes. Most of the 20,000 employees were out of contact with the company. Reaching them, reassuring them, and, where possible, giving them some sense of normalcy became a top priority.

Among the tools employed were the corporate Web site, press releases, and a quickly converted help desk facility with a toll free call-in number. In the month following Katrina, the company authored nearly 20 media advisories, primarily intended for their employees. These provided information to employees and directed them to look at the company Web site for additional information. The site’s emergency information Web page experienced some 67,000 hits in the weeks after the storm. Employees were also directed to call the corporate emergency help line that provided 24-hour disaster relief. The help line workers had, prior to Katrina, staffed six of the sector’s IT
help desks. In the weeks following the hurricane, they handled over 26,000 calls.

Employees in the recovery area, particularly in Pascagoula and Gulfport, needed water, food, shelter, and fuel. As the fear of disease spread, they also required inoculations and, in some cases, medical care. The Information Technology Solutions disaster recovery center in Dallas, guided by Jimmy Morales in Pascagoula, estimated the needs. These supplies were then “pushed” into the affected area using Northrop Grumman’s fleet of corporate jets, as well as a helicopter and a cargo plane. Northrop Grumman employees drove 32 fully supplied recreational vehicles from Dallas to the coast.

Fortunately, some employees in the region were almost immediately available to assist in the recovery. Many were quickly put to work cleaning up the shipyard. Some IT workers quickly became productive after being relocated outside of the disaster area. Planes coming into Trent Lott Field with supplies returned to Dallas with essential Northrop Grumman Corporation employees. Personnel responsible for the sector’s payroll, for instance, were almost immediately flown to Dallas and were able to get checks out with only a single day’s delay. Nevertheless, many banks in the region were closed and other banks soon limited withdrawal amounts or ran out of cash. Northrop Grumman Corporation quickly made special arrangements with Wal-Mart and Western Union to cash employees’ payroll checks. All employees automatically received pay for the two weeks immediately following the storm; employees who actually worked during those two weeks were additionally paid for those hours, as well.

Human resource management, essential for the recovery process, also was a reassuring source of strength. Support to workers and their families was often repaid in increased loyalty with many performing, and growing, far beyond expectations. The crisis management team challenged employees to take on necessary, but often difficult, roles; their trust was usually rewarded. A typical example was an employee whose house was partially destroyed, but a dry second floor was still habitable. Though fuel for his generator was almost gone, he offered to use the last of it to drive to the Pascagoula shipyard to report on conditions there.

While at the shipyard, that employee asked CIO Shelman if he could pick up some fuel and, if available, some food for his family. Shelman immediately agreed but, as he notes, not without raising concerns of the precedent his action might be setting:

“Someone from another area of the company gave me a little pushback for exceeding my authority. I got on the phone to my boss and told him I was calling with two possible purposes, either to resign so I could sell my stock to provide food for those people or get his ‘go ahead’ to feed them. He said, ‘I want you to do everything you can. Do what you would do if they were members of your own family.’”

Transforming Leadership

In the days following the disaster, rapid decision making became essential. Managers were given license to make decisions with far less analysis and oversight than was customary. This leeway required a temporary transformation in leadership and leadership style. Moreover, Ship Systems’ local management was initially scattered and, in most instances, unreachable. Many faced extreme hardships within their families. Those in the disaster area who were willing and able to work did not initially have the resources, particularly communications, to organize a recovery. Moreover, some of the necessary decisions would have far exceeded their authority and scope of operations, even if they had been able to respond.

As a result, the senior managers of Northrop Grumman transitioned during the early days of the recovery from their usual focus on planning, strategy, budget management, and organization structure to focusing on tactics and operations. They became hands-on managers, taking calls from the field or listening to the estimated needs from the crisis team and then, in the next minutes, marshalling specific responses to meet those requirements. One senior manager describes the environment:

“It boiled down to making decisions quickly. Large corporations can easily find themselves going into analysis paralysis in their normal operations. Most of that went out the window as we worked to solve problems at what we soon were calling ‘hurricane speed.’”

Hierarchy tended to dissolve in the face of uncertainty and limited information. In the first days, when Morales called back from Pascagoula to Dallas, he was, as Shelman described him, “the Captain on the Deck” and “our eyes and ears on the ground.” In uncertain times, good information was more important than management position in shaping direction.
The disaster recovery team realized that resources normally provided to them by their primary “customer”, the president of the Ship Systems sector, had become part of Northrop Grumman’s recovery domain. Food, water, fuel, clean power, security and so on, were examples. Morales worked closely with the sector management team for the next month. His charge was to help solve many of those non-IT-related infrastructure issues, thus allowing Ship Systems’ management to concentrate on getting the yards ready for business. But importing relief workers had to be managed with care because they too had to be fed and sheltered.

Managing in a Stressful Environment

Human resource issues presented unique leadership challenges. Stress, already high from the storm itself as well as from the personal challenges the storm created, intensified for some as the magnitude of the recovery requirements emerged. In some instances, that stress led to requests for time off. Sector CIO Jan Rideout, for instance, needed several days to recover from the loss of her home. But senior management recognized the need to transition her and others back into their roles as quickly, yet as compassionately, as possible because they were needed for the Herculean recovery efforts. Management also needed to harness the great outpouring of offers from employees seeking to help. For several days, there was a line of people outside Shelman’s office, waiting to be assigned to do something, anything, to be of assistance.

RESTORING THE IT INFRASTRUCTURE

This disaster far exceeded the assumptions underlying the sector’s business continuity plan. But, the Ship Systems sector did survive, returning to operations just two weeks after the storm. By October 13, six weeks after the storm, 12,500 of the Ship Systems sector’s 20,000 Gulf Coast employees were back at work. Getting IT back up and running was an essential element of this recovery.

Katrina was so vast that it knocked out two Ship Systems data centers that had been assumed to be geographically far enough apart to serve as backup for each other. Assumptions about the availability of public infrastructure also proved overly optimistic. The storm severely disrupted the communications infrastructure in Pascagoula and Gulfport. Switching stations, cellular antennas, and other essential elements of the public communications infrastructure had been swept away. Public communication was disrupted for weeks. Other essential elements of the public infrastructure were too. Electric power, as had been anticipated, quickly failed. And, while some generators were available, there was little gasoline available to fuel them.

Northrop Grumman Corporation was fortunate to have had a partially manned U.S. Navy ship still in the Pascagoula Yard at the time of the storm. Using its satellite communications equipment, Ship Systems personnel who had stayed behind were able to provide the sector president, Philip Teel, with an initial damage assessment. But electronic communication was almost nonexistent due to failures in the public communications infrastructure and the widespread destruction of the communications infrastructure in the Pascagoula and Gulfport yards. One exception was with BlackBerry devices that were, in some instances, able to communicate asynchronously with one another using text messaging—at least until their batteries died. This communication, though, required the sender to have the PIN number of the recipient’s BlackBerry. Unfortunately, a directory of PIN numbers was not available at the time of the storm.8

Reconnecting the Yards

When Morales landed at Trent Lott Field, he brought a number of satellite phones, which were immediately distributed to key members of the Ship Systems management team. These phones were helpful in coordinating initial relief efforts between the yards and the crisis center in Dallas. But these phones, which required line-of-sight access to satellites, were difficult and frustrating to use. Ship Systems sector personnel had to be taught, and sometimes re-taught, how to use them. Within several days, satellite dishes were installed at the Pascagoula and New Orleans yards to provide the necessary bandwidth for both voice and data Voice-over-IP (VoIP). Phones began to arrive and, via the satellite dishes, provided a more robust communication channel.

Early on, it became clear that rebuilding the Pascagoula data center would be impossible. Yet communications tools were needed to recover the yards, and then to return to business as usual. Walkie-talkies were acquired to replace the hundreds of two-way radios previously used for within-yard communication. These walkie-talkies were essential

8 Every BlackBerry is assigned a unique, eight-digit number, called a personal identification number (PIN), which is different from its phone number. With that PIN, text messages can be sent directly to a BlackBerry user’s PIN, even when the e-mail server is not available.
in managing the recovery and reopening of the yards. Reopening actually required new communication linkages to and between the 120 new mobile offices that were being repopulated throughout the shipyard. A plan had already been in place to move to a wireless solution for those buildings, but its implementation was several years away. Wireless offered a quick and fairly inexpensive replacement for the yard’s destroyed communications infrastructure, providing both data and, via VoIP, voice connectivity.

**Building a New Data Center**

Imagine losing 1,500 desktop and computers, nearly 200 servers, and much of your communications infrastructure in a matter of moments! That was the technical and procurement challenge the crisis recovery team faced. And, with both data centers inoperable, Northrop Grumman needed an alternative data center—quickly. Fortunately, as part of an ongoing data center consolidation effort, many of the applications from both shipyards had already been migrated to Dallas. This transfer had made it relatively easy to get out the sector’s payroll with almost no delay.

Dallas was quickly chosen as the site for a new data center. The existing facility had available space; the only missing elements were personnel and equipment. Several employees previously employed at the Pascagoula shipyard relocated to Dallas on Wednesday, two days after the storm. They began the restoration process along with personnel from other sectors.

Because of its size, as well as its priority as a defense contractor and its established relationships with IT suppliers, Northrop Grumman Corporation was able to build, in a matter of just days, a mirror image of its Pascagoula center. On Tuesday, the day after the hurricane, Shelman and his team were on the phone with key vendors. Shelman describes:

“I called the suppliers on day one and told them, ‘You know what you’ve sold us for that facility. Reorder it ... all.’ We wanted to get those orders in quickly. Our contracts with the suppliers called for guaranteed hot shipments, but if the damage was as widespread as I feared, the suppliers would be looking at a huge backlog of orders. How could they fill everyone’s demand?”

The restoration of the data center presented difficult challenges. Servers arrived before the racks that would hold them and were immediately assembled on tables. Later, those servers needed to be relocated, and their cables woven into cable management trays. This relocation required taking the servers off-line for several hours, a difficult challenge when the business was running flat out to recapture lost productivity from the storm. Northrop Grumman’s recovery staff also sometimes encountered incompatibilities between systems software and the new hardware environment, complications that took time and effort to resolve. And, as systems were restored and normal business operations resumed, more and more time was required to handle the normal maintenance requests that were beginning to flow in.

Assumptions about documentation requirements brought unwelcome surprises. While application and system architecture documentation was generally up-to-date, it was not always accessible. For instance, information about product and license keys, server names, addressing schemes, login IDs, and so on were sometimes difficult to find or in the heads of people who were no longer accessible. Some information, carefully tucked away in file cabinets or network administrators’ locked drawers, had fallen victim to the storm.

**Restoring Data and Applications**

One large firm affected by Katrina found about 75 percent of its files backed up from New Orleans to Houston initially unreadable. Northrop Grumman Corporation was in far better shape. Almost no data had been lost, thanks to the sector’s IT disaster preparedness. Backups had been taken and delivered to Iron Mountain, as well as to Dallas. One exception was data for the DDG 1000 extranet, which had been running until its servers were destroyed. But only the data from a few hours before the storm was lost; those users had been made aware of the risk in the hours before the storm touched down. And, while over a thousand PCs were lost, the essential data they accessed was on servers that had been backed up. Arrangements were made to try to recover, at a steep price, essential data that might have been lost on desktop or laptop machines, but very few requests came in.

The crisis team initially found itself in uncertain waters in prioritizing application recovery. The sector’s business continuity plan provided some guidance, but it lacked some important dimensions. For instance, applications that had been identified as essential when the plan had been drawn up were now less critical than getting up e-mail or other elements of the communications infrastructure. And, because of
the DDG 1000’s upcoming design review, recovery of its extranet was of greater importance than had been predicted months before. It was migrated to Dallas and brought up in just six days; the review itself was successfully completed a week later.

**PLANNING, RECOVERING, AND LEARNING FROM DISASTERS**

By September 14, two weeks after Katrina, the Ship Systems sector had a new data center, and the two Gulf Coast shipyards had connectivity and essential systems up and running. Equally important, Shelman’s organization had played an instrumental, and somewhat unanticipated, role in finding and supporting the sector’s employees and their families. His organization had also helped to get the payroll out and distributed, where possible, and get people back to work. Overall, the speedy recovery at Northrop Grumman Corporation can be attributed to planning, but even more to agility, teamwork, and leadership in dealing with the unanticipated.

IS organizations have resources to plan for and recover from a disaster like Katrina. Here are some of those resources.

**Disaster Preparedness**

“The best form of crisis management is preparation.” is the well-worn credo of experts in the crisis field. But can you plan for a disaster of the magnitude of Katrina?

Most organizations make the mistake of preparing for disasters specific to their domain, that is, they prepare for events they believe are most likely and will have the greatest impact on their operations. For example, financial institutions prepare for IT failures, hospitals for pandemics, and airliners for technical failures and sabotages.

An alternative approach is to consider a broader spectrum of disaster types, such as the generic disaster categories of economic, information, physical, human resource, reputation, psychopathic, and natural disasters. While it is impossible to prepare for every conceivable disaster in each category, it is possible to prepare for one in each, thus establishing a “disaster preparedness portfolio.” Disasters in the same category share common characteristics. Preparing for at least one in each category decreases an organization’s overall vulnerability on an infinite disaster spectrum.

Narrower in their scope, but more specific to IT disaster preparedness, are two frameworks that have gained considerable attention recently in the IT field: COBIT (Control Objectives for Information and Related Technology) and ITIL (IT Infrastructure Library). Designed to be open, comprehensive and industry-encompassing, COBIT and ITIL include sections on disaster preparedness and business continuity planning (see Table 1).

COBIT has gained global acceptance as “good practice” across industries; it is understandable to both operational IT and business managers, and it supports the IT auditing process. It is intended to help the IT organization master the three core elements of IT governance: IT as an asset, IT-related risks, and IT control structures. By considering and mostly incorporating established frameworks, such as the Software Engineering Institute’s Capability Maturity Model (SEI’s CMM), ISO 9000 and 17799, COBIT serves as an integrator among disparate best practices and unites them into one generic framework; or at least it provides an open interface to do so. As a complement or part of COBIT, and with a slightly different objective in mind, ITIL’s main focus is to improve the efficiency and effectiveness of IT services delivered to customers within the enterprise. ITIL has become a de facto standard for IT service management.

Both frameworks provide generic objectives and measurements, as well as excellent guidelines for establishing IT disaster preparedness, and both emphasize developing an IT continuity plan, identifying and allocating critical resources, executing a business impact analysis, and maintaining, testing and training of the plan—to name a few.

---

Both frameworks encourage disciplined IT preparedness behavior, but they are rather non-specific and provide only limited guidance on how to take those IT preparedness steps to the operational level.\textsuperscript{5} Also, COBIT’s and ITIL’s exclusive emphasis on IT leaves out planning parameters outside the technical realm. As Shelman’s quote at the beginning of this article demonstrates, assumptions cannot be taken for granted. These assumptions, such as the availability of employees, communications, roadways, and electricity, often form the prerequisite of most continuity plans.

**Disaster Recovery**

Due to their emphasis on IT disaster preparedness, COBIT, ITIL, and other frameworks in the disaster management literature provide less direction on recovery strategies. They presume that the level of preparedness determines the scope of reactivity on hand after a disaster has struck. However, if a contingency plan cannot be applied, as in the initial days at Northrop Grumman Corporation, management must orchestrate the recovery effort from scratch.\textsuperscript{7}

---

\textbf{Figure 1: Comparison Between COBIT and ITIL}\textsuperscript{16}

<table>
<thead>
<tr>
<th>COBIT</th>
<th>ITIL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author</strong></td>
<td>Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>Established in 1994; the most current version of COBIT is version 4, released in December 2005; version 4.1 is expected to be available in April 2007</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Open standard that integrates established frameworks</td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>IT governance and control</td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>IT governance objectives and metrics</td>
</tr>
</tbody>
</table>

---

\textbf{Learning from Disasters or Near-Disasters}

Compared to the amount of time spent on disaster preparedness and recovery, post-disaster or near-disaster analyses receive little attention.\textsuperscript{8} Few organizations conduct post-mortem analyses, perhaps because nobody wants to assign blame for any failures in planning. Of those who do conduct an analysis, few reportedly know how to do it properly.\textsuperscript{9} Neither COBIT nor ITIL offers guidance.

There are two compelling reasons for post-disaster or near-disaster analysis. First, as noted, organizations can only prepare for a portfolio of crises, not for all crises. To foster and strengthen their future preparedness, organizations need to prepare for unanticipated crises, which they can do by learning from unexpected events or crises that were barely missed.

Second, experts agree that the nature of disasters shifts with time.\textsuperscript{20} The ever-increasing complexity of technology in post-industrialist societies is one cause. Increased complexity shifts the type of disaster toward a “built-in” disaster, raising the likelihood of

---


Societies’ increased dependence on computers and communications systems is a compelling illustration. Global warming and terrorism are two other illustrations of threats whose threat levels have changed over time.

One suggestion is to create a disaster team that is part of a “crisis closedown operation.” Its purpose is to immediately document the experiences of individual disaster recovery participants. This record becomes part of the documented, organizational history. It is accessible by subsequent crisis teams, which could trigger improvements in future preparedness efforts.

With the objective of using the Northrop Grumman Corporation recovery efforts to provide a record for other preparedness efforts, we provide the following lessons learned from interviews conducted with key players of the recovery effort.

TEN LESSONS FROM NORTHROP GRUMMAN CORPORATION

After the recovery was complete, Northrop Grumman carefully evaluated the effectiveness of its emergency preparedness and response. It drew the following ten lessons from its experience.

Lesson #1: Keep Data and Data Centers Out of Harm’s Way

The Ship Systems sector had a business continuity plan, as did all the other Northrop Grumman business units. But at least one planning assumption—the separation of backup data centers—did not reflect either the scale of Northrop Grumman or the scale of the hurricanes in that part of the country. Ship Systems sector’s policy designated that backup data centers had to be located at least 100 miles from the site they were backing up. But Katrina’s width exceeded this planning assumption and knocked out two centers designated as backup sites for each other.

At the time of the storm, management was considering data center consolidation across the firm. That plan would have eliminated all but seven centers, leaving only one in the Gulf Coast. Since the storm, consolidation has been revisited. There will now be four centers. None will be in the Gulf Coast or locations threatened by hurricanes, earthquakes, floods, or other natural disasters.

Lesson #2: Don’t Assume the Public Infrastructure Will Be Available

Most IT disaster planning documents assume that public communications will survive, when, for instance, there are two independent communications pathways into a facility. But Katrina took out all public communications. Moreover, as the Northrop Grumman experience illustrated, the problem went well beyond communications. Roads were washed away or closed by authorities, airports were inaccessible, water was shut off or polluted, food, fuel, and other supplies were unavailable, police looked after their own families, and so on.

As Northrop Grumman Corporation experienced these problems, it adapted to them on the fly rather than reference plans. Its leadership in crisis is an inspiration to future planners. Today, its disaster preparedness plans include the vulnerability of the public infrastructure. As a result, extra satellite phones are now in secure locations, and satellite dishes can be safely sheltered and then redeployed after disruptive events.

Lesson #3: Plan for Civil Unrest

The major problem the company faced in New Orleans was access to its facility. Real, exaggerated, and imagined threats of civil unrest led to a near lock-down of Jefferson Parish, home of the New Orleans shipyard. Management therefore decided to bring in personnel from outside the area to secure the facility. Disaster preparedness can include contracting for such services and planning how security personnel will be notified, transported, fed, and supported during the period of threat.

Lesson #4: Assume Some People Will Not Be Available

Business continuity plans often assume that employees will be at the site of the disaster to initiate and execute the IT recovery plan. Northrop Grumman Corporation was fortunate. Due to its size and geographical reach, skilled employees were available and could quickly be called upon for the recovery effort. The company also benefited from the voluntary relocation of some of its staff who knew the Pascagoula data center and its suite of applications well.

Where knowledgeable people were not available, Northrop Grumman’s disaster recovery team called on employees with little computing background to turn servers on or off, configure VoIP phones, and perform other IT work. When the A-team was unavailable, the only viable alternative was to assemble a B-team. Since Katrina, Northrop Grumman Corporation has established backup role takers for all key personnel.

Lesson #5: Leverage Your Suppliers as Critical Team Members

Northrop Grumman Corporation’s primary IT suppliers — AT&T, Cisco, EMC, Hewlett Packard, IBM, KST Data Inc., Nextel/Sprint, Oracle, RIM, Skycasters, Sun Microsystems, and others — were extremely responsive in providing equipment and services. Personnel from several of these suppliers became essential members of the virtual team tasked with equipping the new Dallas data center. They expedited deliveries and worked side-by-side with Northrop Grumman staff in assembling and testing the new servers.

Implementing a contingency plan is closely linked to suppliers’ capabilities. Assessing damage quickly and getting orders to suppliers can reduce bottlenecks in your supply chain, particularly if other firms are also clamoring for replacement equipment. Fortunately, while Katrina was a regional disaster, the hardest-hit section of the Gulf Coast had a relatively sparse information technology footprint. Thus, hardware vendors did not face sudden overwhelming demand, which might have occurred, for instance, if such a hurricane had hit Houston or a major earthquake had struck Los Angeles.

Lesson #6: Expect the Unexpected

All contingencies cannot be planned for. Even if all possible threats could be identified, it makes no economic sense to do so. It is, however, possible to build a “crisis portfolio” by preparing for at least one disaster in each crisis category, as noted earlier.

When we began this research project, one local CIO who had been lightly affected by Hurricane Katrina, cautioned us that the Northrop Grumman story was just too out-of-the-norm to be relevant to most CIOs. Unfortunately, this thinking is exactly what crisis management is all about: plan for the unthinkable. Moreover, the larger the firm, and the more widespread its operations, the more likely it will face a disaster from outside of its organizational boundaries, and thus, outside of its business continuity plan.

Lesson #7: Get Prepared

Besides building a “crisis portfolio,” plan processes to deal with unplanned events. Perhaps use COBIT or ITIL, as noted earlier. Identify crisis teams in multiple locations, define roles, and identify likely role holders and backups. Train and test scenarios. List supplies most likely to be needed, and identify suppliers. Agree beforehand on exceptions to procurement policies during states of emergency. Include in the contact list the telephone numbers, e-mail addresses, and other contact information of people outside the potential disaster area who might assist in locating missing personnel. Inform employees how to call in, before a disaster hits.

Documentation, simplicity, and consistency help backup teams get in place quickly. By ensuring, in advance, that systems are documented completely and simply, the B-team can initiate IT recovery, if necessary. Instructions for the team should describe, in detail, which systems to restore, the order in which they should be restored, and how to restore each one. The documentation should be written and tested with the assumption that the user has no context-specific information other than what is provided in the documentation. In some cases, for instance, for server shutdowns or restarts, assume little or no technical knowledge. Furthermore, to reduce risk and simplify restoration, have consistent standards and procedures across common elements of work (e.g., naming conventions, server installations). Perhaps most importantly, consider simulating a disaster, evaluating the responses, and modifying your plans accordingly.

Lesson #8: Establish a Strong Leadership Position

As noted earlier, if the assumptions underlying a disaster recovery plan fall far short of the actual event, then the disaster recovery is more about reacting to the situation at hand than executing a pre-defined plan. Therefore, use the disaster recovery plan as a model. But be flexible in allowing leadership skills to transcend an inadequate plan. Acting quickly (at “hurricane speed”) and decisively prevents the organization from falling into analysis paralysis. Decisions must be made fast, under high levels of uncertainty. There may be no time for a committee discussion. Decision makers may have to fall back on their instincts and leadership experience.

To reduce uncertainty, communicate liberally and continually to fill the information vacuum that occurs
following disasters. Sharing facts stimulates the flow of feedback from disparate, disaster-affected key constituents, which, in turn, increases the quality of information for decision making.

Lesson #9: Empower Decision Makers on the Team

Often, pre-established decision hierarchies dissolve in crises. In addition, leadership becomes more centralized and more decentralized, simultaneously. Leadership becomes more centralized because the high level of uncertainty and the need for rapid reaction leaves no choice. Leadership also becomes more decentralized because communications break down and local action must proceed anyway. With first-hand knowledge and the necessity to execute, people at the disaster scene often must exceed their prior authorities and operational scope to move the recovery effort forward.

Lesson #10: Exploit Fresh-Start Opportunities

On the bright side, a destroyed hardware infrastructure can provide the opportunity to upgrade the equipment—an opportunity that might not otherwise be cost-justifiable. Prior to the storm, Northrop Grumman Corporation planned to consolidate its data centers. Hurricane Katrina accelerated and reshaped that plan. Similarly, the implementation of VoIP and wireless connectivity within the shipyards was accelerated. All resistance to the upgrades evaporated. They had to be done. With this new communications infrastructure in place, novel applications, such as equipping engineers with wireless handheld data entry terminals, could be justified without having to include the cost of the new wireless infrastructure. That investment had become a sunk cost.

CONCLUSION

“I’m not as concerned about another storm like Katrina; we are far more ready today than we were then. We have satellite dishes and phones ready to fly in; we could set up communications in half, maybe a tenth, the time. Our new data center consolidation plan will ensure our data will be safe from natural disasters, such as earthquakes or hurricanes. More importantly, our business continuity plan is now squarely focused on our people, as well as our systems.”

As Shelman notes, Northrop Grumman learned a great deal from its experience with Hurricane Katrina. Foremost, it acknowledges that disasters happen and will continue to happen. Thorough and methodological preparedness planning is essential, but the assumptions underlying these plans must be carefully considered. Assumptions regarding disasters will not necessarily match the actual disaster, so staff knows it will need to be flexible and adaptable when responding. The company is regularly testing, evaluating, and reconsidering its plans, knowing that these plans are imperfect and will provide only a rough guide to recovery. The value of post-disaster analysis is also recognized.

Preparedness extends beyond individual firms and first responders. The world needs planning to deal with crises using our increasingly important data highways. How can our national and international resources be safeguarded from cataclysmic disruption and, if such disruption should occur, how can we quickly recover? The electronic infrastructure underlying so many aspects of modern life places a major responsibility on all levels of government to be more prepared than past disasters, such as Katrina, have shown them to be.

ABOUT THE AUTHORS

Iris Junglas

Iris Junglas (ijunglas@uh.edu) is an Assistant Professor in the Decision and Information Sciences department at the University of Houston’s C.T. Bauer College of Business. Before receiving her Ph.D. from the University of Georgia, she worked as a consultant for PricewaterhouseCoopers. Her research has been published in various IS journals, such as e-Service Journal, International Journal of Mobile Communications, Communications of the ACM, Information Systems and E-Business Management, and the Communications of the AIS.

Blake Ives

Blake Ives (blake.ives@uh.edu) holds the C.T. Bauer Chair in Business Leadership at the Bauer College of Business at the University of Houston. He is also Director of the Information Systems Research Center (ISRC) and Director of Research for the Society for Information Management’s Advanced Practice Council. Blake is a Past President of the Association for Information Systems, a Fellow of the Association