Disaster Recovery and Business Continuity Planning:  
A Case Study of an Incident at ABC Corporation

Jared Spencer  
Nova Southeastern University  
sjared@nova.edu

1.0 Introduction
Risk management is a broad topic that spans several stages and encompasses a range of measures that must be evaluated. Once the risks to the organization have been identified and understood, the next step in the process is choosing a strategy for dealing with those risks. A number of control strategies exist for defining how and developing a structure to address risks (Cannady, 2005; Peltier, 2005). Most risks require some form of mitigation, or approaches to minimize the exposure.

Incidence Response Planning (IRP), Disaster Recovery Planning (DRP), and Business Continuity Planning (BCP) provide methodologies for dealing with incidents or disasters in the immediate, short-term, and long-term time frames respectively (Cannady, 2005). An organization seeking to protect and ensure continuing operations in the face of such situations would need to evaluate each of these phases and establish an appropriate course of action should an incident arise.

Peltier outlines a number of measures that can be taken to study the effectiveness of a mitigation plan (2005). Many of the measures inherent in evaluating these plans are qualitative. As such, a case study presents an excellent means to not only gain further insight into a given mitigation strategy, but to expose potential weaknesses and identify areas for strengthening the plan.

2.0 Problem Statement
This study represents a component of a broader, ongoing security evaluation of a global technology organization. In this phase of the research, the company’s mitigation strategies will be evaluated in the context of a real incident that impacted the availability of the site’s physical location and equipment. The actual events that took place, as well as the company’s response to those events, will be presented and evaluated. The goal will be to evaluate the events of an actual disaster so that organizations of comparable size and nature may better position themselves for similar situations.

3.0 Background
The global technology organization being reviewed in this study is a well-known provider of Information Technology products and services, with offices throughout North America and the world. The site of the study is an office in a major metropolitan center in North America. This location is small in relation to other company offices, with a staff of a few hundred people – mostly software engineers for various product lines.
Given the sensitive nature of security, the company will only be identified as ABC Corporation, or just the company. Other identifying information will be masked throughout the course of the study, including participant names, organizational units, and unique software products. The site of the study will be hereafter referred to as the local site or office.

This researcher has been given access by appropriate managers at the local site to study security measures in place and interview staff members who work in security-related capacities. Primary among these is Mr. B. Mr. B is responsible for many of the security initiatives implemented at the local site, and also works closely with the CIO’s office and corporate security team to ensure that company-wide directives are in place and being followed appropriately (Spencer, 2005).

The incident being presented in this study began on August 17, 2005 when a major water main burst, flooding much of the downtown area in the vicinity of the local office. While the local office itself did not sustain any direct damage to its office or technology equipment, water service was affected, and the chilling fans that provide air conditioning service were left underwater and unserviceable. The days of mid-August are the hottest time of summer in that region of the country, and the offices soon became inhabitable. Concerns rose about computing equipment and other facilities which led to a large number of machines being shut down. Employees were not able to come to the building due to the heat and safety concerns related to medical facilities and sprinkler systems. Early estimates were that the chillers would be out of service for a minimum of two weeks.

Ultimately, the outage ended up being shorter than predicted. The early estimates for disruption were overstated, and air conditioning service was, in fact, restored in less than a week. Nonetheless, during this time, a disaster was taking place, and all local site employees and management had every reason to believe it would last for weeks. This study will focus on the events that took place in the days beginning on August 17. Some of the actual communications will be presented, as well as results of a questionnaire provided to Mr. B. The goal will be to evaluate the mitigation plans in existence at the local site, and their effectiveness as they were implemented during this crisis. Weaknesses will be exposed and proposals offered to address them.

4.0 Methodology
4.1 Incident Development

The water main break occurred in the morning hours of August 17, 2005. Local news media were covering the story, and many employees at the site became aware of the situation through early reports. The break occurred 6-8 blocks away from the location of the local site; so although there was an immediate disruption in water service, there was not any early indication what the longer term impacts, if any, would be. A message sent to local site employees on this date reflected that local site management initially believed that the problem would be short-term (Facilities group, personal communication, August 17, 2005).

As the day progressed, the magnitude of the break began to unfold, and it became clear that there were going to be more significant ramifications. At this point, no disaster measures had been implemented, as it still appeared as though the impact would be short-term. By early afternoon, it was discovered that the sprinkler systems might not function. Although there was never a forced evacuation of the building, at this point employees were strongly urged to leave. A message sent to all local site staff indicated that, in addition to the
potential problems with the sprinkler systems, local emergency services were being impacted, and safety concerns existed for anyone remaining on the premises (Facilities group, personal communication, August 17, 2005).

The nature of the work conducted at the local site is primarily development and technical support. Some staffers work directly with customers and on-site consultants in a problem resolution nature. This would strongly suggest that any outage lasting more than a matter of hours should trigger disaster recovery actions. However, the ABC Corporation does not look at the situation in the same light.

In response to questions posed by the researcher, Mr. B clearly states that there is no site-wide disaster-planning requirement (Mr. B., personal communication, September 13, 2005). Although a representative from the local security team is responsible for coordinating the efforts, ultimately each individual group is basically on its own to determine how to respond in a crisis. This concern is covered in greater detail in later sections. With the possible exception of some individual group activities, no disaster-recovery actions were taken on the initial day of the outage.

4.2 Disaster Realization and Actions Taken

By the beginning of day two, or the day following the water main break, it was becoming clear that there was a greater challenge facing the local site. The chillers that provide air conditioning service were entirely submerged, and all indications pointed to at least two weeks of downtime before repairs could be made.

As the issue with air conditioning began to develop, critical equipment in the central lab was shut down to avoid overheating. Air conditioning the central lab is maintained, at least in part, through separate equipment, and it was able to be returned to partial operating capacity in a matter of hours. However, due to concerns that this capacity might be insufficient to cool the environment if all machines were operational, it was recommended that non-critical equipment be left off.

As such, the developing situation by day two was that the temperature in the local site facility had continued to climb, and when levels of 85 degrees and higher were reached, the building had basically become inhabitable. With a potential outage of two weeks or longer, clearly there would need to be actions taken to provide a means for employees to continue to work. As noted earlier, however, no site-wide disaster recovery mechanism existed.

Because of this, the actions taken were unclear and uncoordinated. Site executives discussed the situation with managers from a nearby ABC Corporation office in an effort to arrange alternative facilities for employees to work. Ultimately employees were given the opportunity to work from this alternate location, provided that site was able to accommodate all those who needed to do so. This location is relatively small and only has the capacity to house a portion of the local site staff. The site executive at the alternate location, however, did offer the limited facilities that were available for use by the local site staff if needed (ABC Corporation Site Executive, personal communications, August 18, 2005).

This offer was provided to local site employees on a group-by-group basis, and they were allowed to decide at their own discretion whether to use these facilities. The managers of each group were attempting to determine how to best keep their respective teams functioning. These efforts were scattered and there did not seem to be a coordinated effort to determine how to proceed.
During this period, most employees chose to work at home if they had the needed equipment and their responsibilities allowed them to do so. By Friday, August 19, no formal plans had been communicated (nor developed, to the knowledge of this researcher). With the arrival of the weekend, many employees would be off; however, challenges remained for those on call or who had responsibilities during this time.

The on-call procedure at the local site is handled, for most groups, by means of an automated process that runs on a machine in the central lab. This process watches a queue for new issues and, when one arrives, automatically issues a page to the appropriate device. However, this machine had been powered down as part of the precautions taken to protect equipment from the rising heat. Thus, while this machine was off, on-call staff members had no way to determine if new issues had been reported, and no procedures existed for how to handle such a situation. As such, those on call were asked to log into the issue management system at least once every hour to manually check if any new problems had been reported. This, clearly, was not an optimal solution. To add insult to injury, on-call staffers were not even given the opportunity to discuss this situation. Voice mail messages were left by managers (at least in the one case that this researcher is aware of) on the cell phones carried by those on-call with the aforementioned instructions.

4.3 Problem Conclusion

By Monday morning, in surprise news, the problems had been resolved. It was unclear how or why the early predictions were so far off the mark, but over the weekend the water submerging the affected equipment had been pumped out, and the chillers were dried and returned to operation. Mr. B reported in an email to employees on Sunday that temperatures in the building were dropping and would likely be back to normal by start of business Monday. Most employees returned to work on Monday, August 22.

Thus, the duration of the crisis at the local site was approximately three business days and five days total. During this time, machines and equipment were unavailable, and the premises were largely inhabitable. The following sections will look at the effectiveness or lack thereof of the local site’s response to this incident, and actions that may be needed to improve the readiness for future disasters.

5.0 Barriers

As noted previously, the incident that affected the local site of ABC Corporation lasted for roughly three business days, and five total days. As noted by Mr. B (and discussed in more detail in later sections), the local site does not perform processes that are deemed critical by the corporation. Thus, there was no opportunity to observe the full-scale deployment of a disaster recovery plan. Nonetheless, this researcher was able to witness and document the events that took place, as well as the efforts to provide continuing business operations during the incident. With the outage initially expected to last for as long as two weeks or more, the actions can be analyzed from the perspective that everyone involved believed that a long-term outage was beginning, and the plans implemented should have reflected that belief.

The other barrier worth noting is that, while Mr. B is an integral part of the security process at the local site and provided the researcher with detailed information regarding the outage, there may have been meetings and decisions taking place at management levels that
neither the researcher nor Mr. B were aware of. If this were the case, it would have been relevant to include those details into the case study. However, there was no evidence available to this researcher that such meetings or decisions ever took place; and, regardless, they would only offer to support the conclusions that will be presented.

6.0 Conclusions

Several problems can be identified by reviewing the events that took place at the local site during the days of this incident. First and foremost among these is the lack of a centralized disaster strategy at the local site. Mr. B was quoted in earlier sections on his comments regarding the company’s belief that the local site does not include any “Vital Business Processes.” This is certainly a huge concern. It would seem to be the type of thinking that is clichéd of the organization that can’t see past the bottom-line importance of sales interests. Interestingly, however, this issue may have recently been brought to light – not only by the outage, but from a previous corporate security evaluation, which was discussed by this researcher in an earlier study of the local site (Spencer, 2005). Mr. B. commented that disaster strategy was an area identified in the recent security evaluation as being one where the local site needed to be stronger (Mr. B, personal communications, September 13, 2005).

It would be beyond the scope of this study to expand upon the specific steps that would be necessary for the local site to implement an appropriate, centralized disaster strategy. However, it is worth noting that this researcher, many months back, was a member of a team that was tasked with developing, with the aid of a specialist from the ABC Corporate disaster planning team, a disaster planning document. Unfortunately, however, this effort never reached fruition.

As part of a comprehensive disaster plan, the local site also needs to have arrangements in place for the use of off-site facilities. This need has apparently been studied in the past with less than positive results. Mr. B reported in response to the researcher that past efforts had been made to arrange for alternate facilities to house both staff and equipment in the event of a disaster. However, these plans had been vetoed by management due to lack of space at the alternate locations (Mr. B, personal communications, September 13, 2005).

Another interesting point about these concerns is the diligence by which the local security team handles other security-related matters. As an example, the backup strategy employed by the local site and reviewed by this researcher is sound and thorough. It includes a combination of full and incremental backups that spans a period of months. Tapes are regularly stored in a secure off-site facility. It seems to this researcher to be a paradox that other functions of security are addressed so thoroughly, while issues surrounding disaster planning are seemingly ignored.

The other issue identified by this researcher was one regarding communication. While there were a number of email messages sent during this period, it was quite unclear who, if anyone was in charge. This is likely compounded by the fact that the local site does not have a “site executive,” or someone who is in charge of all site operations. An executive at a nearby location of ABC Corporation actually holds the title of site executive for the local site as well. At any rate, emails containing information and guidance were sent from Mr. B, representatives of the facilities department, at least two local executives, department managers, and the site executive (from the remote location). Through all of these, it was
unclear who was “calling the shots” regarding the outage. With no comprehensive disaster plan in place, it would seem that the appropriate leaders would need to come together and critical decisions be made on how to continue operating the business. But, as noted earlier, there was no evidence to this researcher that any such meetings took place.

7.0 Results / Lessons Learned

Time will tell if the local site will learn from this experience and put forth the needed effort to develop a comprehensive disaster plan. While this outage did not turn into a true crisis, it seemingly could have quite easily; the situation clearly demonstrated that plans need to be made to prevent a site disaster from turning into a business disaster.

This researcher believes that there are lessons for not only the local site, but the corporation as well. The policy that deemed the local site to not house business critical processes does not seem to be well-considered. Without further study of the policy itself, it does present the question of what constitutes business critical processes. Is it only when sales staffs are involved? The failure to include engineers who often work directly with customers and on-site consultants would seem on the surface to be short-sited. It also seems to be somewhat of a contradiction when the corporate policy states that a comprehensive disaster plan is not required, yet the results of a security evaluation (initiated by the CIO’s office) suggests that one needs to be in place.

Ultimately, this study has found that the local site of ABC Corporation is weak in disaster preparedness. If steps are not taken to rectify the problem, it is only a matter of time before this weakness is exposed with ramifications far worse than those reviewed in this incident. For similarly-positioned organizations, this study exposes the potential vulnerabilities created by underestimating the importance of “non-strategic” activities, as well as the criticality of centralizing disaster planning and developing site- and/or company-wide response measures.

References

