Global Information Assurance Certification Paper

Scott Hannig
September 21, 2001

SANS Security Essentials
GSEC Practical Assignment Version 1.2e

Recovering From Disaster:
Implementing Disaster Recovery Plans Following Terrorism

Introduction: The biggest disaster of our time

The necessity for solid Disaster Recovery Plans has never been as evident as it is now, following the biggest disaster ever known to the American people. On September 11, 2001, America was brutally attacked by terrorists, and "security" became more important than ever, in every aspect of living. Following the collapse of the two World Trade Center Towers, and the horrific explosion in the US Pentagon, several businesses and government agencies had to act quickly to begin implementing the carefully thought-out disaster recovery plans that they had previously established to ensure business continuity and strengthen security. Fortunately, many of the companies were prepared with well-designed Disaster Recovery Plans and were up and running by the following Monday so that corporate America could continue to thrive.

Purpose

The purpose of this paper is to examine the process of disaster recovery following the biggest disaster in American history. More specifically, three aspects of disaster recovery, which were found to be the most challenging for many of the companies affected by the recent attacks, will be discussed. These three aspects are:

1. Accessing the needed software and technology
2. Staying connected with employees and customers
3. Loss of valuable personnel

Reasons for difficulties will be addressed, as well as ways in which these difficulties were handled to make the disaster recovery procedures run smoothly. Suggestions for future disaster recovery plans will also be included.

1. Accessing the needed software and technology

Difficulty: High volume of businesses needing help at the same time

In the days following the attack, business recovery centers and hardware vendors were inundated with disaster declarations and requests for help from the hundreds of businesses affected by the collapse of the World Trade Centers. According to a recent article by Carol Sliwa, 73 disaster declarations from 36 companies were fielded by Comdisco Inc., alone, by Friday, September 14. Additionally, not only were there an unusually high amount of requests for help, but the recoveries were the most "complex and challenging" in history, according to John Jackson, the president of Comdisco's availability services group.

Hardware vendors, such as Dell Computer Corp. and Hewlett-Packard Co., were also extremely busy serving customers affected by the attacks in the days following. A recent article by Jaikumar Vijayan reported 80 of Dell's major clients located in the World Trade Center Complex had contacted the Corporation by Thursday. They received orders for nearly 5,000 laptops, desktop computers, and servers. Because of the large volume of requests coming in, both Dell and HP implemented a priority-based system for shipping out equipment, with government and health care customers being first on the list. Thus, financial businesses may have had to wait for their equipment to be shipped. In addition to hardware, requests were also being made for help setting up equipment, and for temporary space.

Solutions:

Some businesses have avoided the problem of accessing equipment by contracting out contingency planning to specialized firms, who have been able to provide them with their needs. According to Sliwa, these firms are able to "completely reconstitute a company's front-office and back office systems and provide office space in location out of harm's way." Other businesses have their own disaster recovery teams in-house who have managed to create back-up satellite offices complete with desk space for crucial employees, with all data backed up from the main server.

Currently, the overwhelming number of requests for equipment is being well handled by the vendors. In addition to running on a priority-based system, they are also establishing crisis centers, support web sites (such as the Sun Support Forum Recovery Assistance Web sit that has been set up by Sun Microsystems Inc.), and utilizing temporary spaces near their facilities to set up call centers. In a recent article, Melissa Solomon reported that additional help is also coming from volunteers from the IT Community around the country. Besides donating money to relief efforts, IT volunteers offered everything from fully equipped office space staffed with support volunteers to free email services for businesses housed in the World Trade Center.

Difficulty: High costs of replacing hardware and related technology

The cost of rebuilding what was lost is enormously high, which may cause some companies to find themselves in financial difficulty. In his article, "The Toll of Terror on Wall Street," Lucas Mearian reported that companies will have to spend an estimated $3 billion to $5 billion to rebuild and/or replace the portions of the IT infrastructure that were destroyed.

Solutions:

Most major businesses invest in insurance to cover such expenses. However, even with insurance, expenses will still be high. As mentioned earlier, a cheaper alternative chosen by many businesses is to contract out work to a third party. Software systems firms, such as Gaurdian IT, offer recovery centers in which clients can by office space with computers and telecoms systems.

2. Staying Connected with Personnel and Clients

Difficulty: Many people could not contact their employers, employees, and/or clients during the time of the disaster

High volumes of telephone calls made during and shortly after the attack made telecommunications very difficulty on September 11 with both landlines and cellular telephones. In addition, due to the closing of airports, several businessmen and women were stranded in various parts of the country for days, unprepared for work outside of the office. Such people often had only a cellular telephone to communicate with their coworkers and clients, thus making work during this time very difficult. Matt Hamblem reported one example of this difficulty in his article, "Staying Connected in a Post Attack IT World." Hamblem wrote about one woman who was stranded in Los Angelos with only a cell phone, since she was only expecting to be in LA for one day during a conference, which was eventually cancelled. Although she was able to use her cell phone to communicate with her office, she was not able to do any of the work she was used to doing, nor could she use email.

Solutions:

According to Hamblen, analysts are recommending now, more than ever, that IT managers insure that critical employees have multiple ways to reach the office while traveling. Thus, in addition to cellular phones, employees should have a data connection, such as a Research In Motion (RIM) email device. Many employees depended on their laptop access via dial-up connections and security software to allow them to continue working despite their stranded situation. Instant Messaging services also were helpful in keeping people in touch during the times of increased telephone traffic.

Another solution to this problem is still new, but some are saying it is the best answer to keep employees connected. In a *Computerworld* interview with Mitch Betts, two IBM consultants reported on the benefits of wireless LAN technology. Although it is still a rather new and expensive technology, the consultants report that it is easy to install, flexible to accommodate office moves and meetings, and it is very secure.

3. Loss of Valuable Personnel

Difficulty: Terrorist attacks on America have stolen the lives of American citizens

The most devastating, overwhelming, and heartbreaking loss faced by corporate America is that of the valuable, irreplaceable employees who were killed in the tragic events of September 11. This is by far the most difficulty problem for businesses to address.

Solution:

There is no easy solution for such a horrific problem. Therefore, it will always remain a problem during such disasters, even with a strong disaster recovery plan. However, there are some ways which this problem may be addressed in a disaster recovery plan, such as educating multiple employees about the responsibilities of other employees, and having executives' offices in various locations. As with all of the disaster recovery process, redundancy is the key.

General Guidelines for Successful Disaster Recovery

Assumptions

When a disaster recovery plan is created and implemented certain assumptions must be made in order to successfully execute the devised plan. For example if a natural disaster occurs within a certain geographical location, the plan might assume that the disaster does not affect the hot site that serves as the IT department's recovery operations center. The plan might also assume that various financial and human resources are available. Another assumption might be that the needed equipment is available. In the first section of this paper, it was mentioned that Dell and HP had to implement a priority-based system for shipping out equipment, with government and health care customers being first on the list.

Business Impact Analysis

A business impact analysis should be conducted to know a system or application's downtime tolerance for the organization. All systems and

applications that can experience little to no downtime should be identified and proper measures taken to ensure that these systems or applications are backed up to possibly online disk storage at an offsite location.

Backup Procedures

In any organization, written backup procedures and recovery policies must exist. These policies and procedures should be formally documented and documentation standards should exist in order to keep policies and procedures current and up to date. Backup policies and procedures should be read by all appropriate parties, and reviewed and updated on a periodic basis. Additonally, Backup logs should be kept and reviewed on a regular basis. All backup failures and restorations from a backup should be noted in the log. This may help identify and prevent future backup problems.

Information residing on individual PCs, especially sensitive, critical information, should be backed up on a regular basis. Full daily backups or online disk storage may not be as necessary per se mission critical systems or application, but should be backed up incrementally, either daily or weekly, as is appropriate for business needs. Backup tapes should always be rotated to an off site location for storage. In the event of a disaster, the unavailability of backup tapes may significantly affect restoration activities. Redundancy such as this is what saved many of the businesses affected by the September 11 terrorist attacks.

Additional Recommendations

Following the attacks, analysts from Gartner Inc. offered some suggestions for the reevaluation of disaster recovery plans, as reported in an article by Nancy Weil. The following is a summary of some of the recommendations that were made in a recent teleconference:

- Get alternate email addresses for employees
- Distribute “wallet cards” with information about what to do in case of an emergency
- Create a designated place for evacuated employees to assemble in the case of a disaster
- Include local, state, and federal employees in disaster recovery planning

Conclusion

As America continues to rebuild itself following the biggest disaster it has ever seen, those organizations with well-planned, thoroughly-tested disaster recovery plans are carrying on with business – maybe not quite “business as usual,” but

business, nonetheless. Challenges were presented, and most were handled, both by the companies themselves, and by the efforts put forth by others, such as the hardware vendors, software systems firms, and even the volunteers from the IT community. September 11, 2001 was a horrific day of disaster in the United States. However, terrorist attacks will not end life in America as we know it. We will pick ourselves up, dust ourselves off and continue living in the land of the free and home of the brave.

References

Betts, Mitchell. "The wireless LAN's day has come." *Computerworld*. September 17, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63752,00.html (September 20, 2001).

Hamblen, Matt. "Staying connected in a postattack IT world." *Computerworld.* September 18, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63991,00.html (September 20, 2001).

Mearian, Lucas. "The toll of terror on Wall Street." *Computerworld*. September 14, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63919,00.html. September 20, 2001.

Sliwa, Carol. "IT disaster declarations flood business-recovery centers." *Computerworld*. September 17, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63935,00.html. (September 20, 2001).

Solomon, Melissa. "IT community steps up to volunteer." *Computerworld.* September 17, 2001. http://computerworld.com/cwi/stories/0,1199,NAV65-663_STO63941,00.html. (September 20, 2001).

Vijayan, Jaikumar. "Hardware vendors moving to help IT hit by attacks." *Computerworld*. September 14, 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63921,00.html. (September 20, 2001).

Weil, Nancy. "Gartner: What companies should do now." September 17, 2001. http://www.idg.net/idgns/2001/09/17/RECOVERYGartnerWhatCompaniesShould.shtml. (September 20, 2001).

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event