https://doi.org/10.48009/2_iis_2009_529-535

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Jesse Patterson, Texas A&M University – Kingsville, jwpatterson@stx.rr.com
Richard A. Aukerman, Texas A&M University – Kingsville, kfraa00@tamuk.edu
Jack D. Shorter, Texas A&M University – Kingsville, kfjs000@tamuk.edu

ABSTRACT

Disaster Planning involves everyone and everything in a business or organization. This includes: determining which potential disasters might happen to the business, planning how to stay in business should one of these disasters occur, and deciding what employees will need to know in order to make the recovery process as painless as possible.

Keywords: Business Continuity, Disaster Recovery

INTRODUCTION

According the Department of Homeland Security, the number of declared major disasters has nearly doubled since the 1990's as compared with the 1980's. The website for the Department of Homeland Security's disaster preparation, www.ready.gov, also tells us that because the nation's economy is rooted in businesses, business continuity planning and crisis management will help to ensure that the country, the economy and its citizen will survive a major disaster. Examples are the terrorist attacks on September 11, 2001, the Oklahoma City bombing in 1995, and the 1993 bombing of the World Trade Center. [2]

The scope of business continuity planning and disaster recovery planning is massive. This is partially due to the range of crises that can occur to a business. These disasters can include (but are not limited to) hurricanes, earthquakes, floods, lighting strikes, terrorist attacks, data loss, hardware failure, physical theft, cybercrime, weak or non-existent security and recovery policies, and employee incompetence. The solutions to these problems are just as varied and complex, although some basic principles can be applied to every situation. Hardware must be secured, software must be hardened, effective policies must be drafted, employees trained, and buildings prepared (to name a few). Because the field of business continuity and disaster planning is so vast, this paper will focus on what businesses and organizations can do to protect their people, their data and their equipment in the event of a major crisis.

DISASTER PLANNING AND PEOPLE

Employees are the greatest asset to any business. Unfortunately, they are also the greatest liability. While it is true that hardware can fail, and a natural disaster can destroy the very building in which a business operates, it is a far more common occurrence that a careless or corrupt employee will do something (or not do something) that will ultimately destroy the business for which he or she works. The best way to prevent such disasters from destroying a business is to craft a plan, communicate that plan to employees, and ensure that those employees know exactly what is expected of them should a disaster occur. The first step of this plan is to create it, and this is best done by involving those employees who will be affected by a disaster (meaning everybody).

USAA's Plan

Daintry Duffy, a writer for the magazine CSO, relates how one Chief Information Officer, Steve Yates, worked to create and implement a business continuity and disaster recovery plan for USAA. When Yates first joined USAA, he discovered that the only plan the company had for business continuity and disaster recovery was the one printed on paper. Yates didn't know how many people had read that plan, or were even aware of its existence. Before Yates came to work at USAA, the top level staff would gather every year or so in a conference room to role play through the different scenarios that might affect the company. During this role playing, the senior staffers would discuss the procedures described in the written plan and deliberate on how they thought the other employees would respond to those plans. [3] The article also mentions that the only live exercises performed at USAA were periodic data recovery tests of a sampling of business units. For example, the company would select a section of data out of the life insurance department and then recover the data from previous backups. One major question troubled Mr. Yates: "Could the company really withstand something massive instead of minor?" When the terrorist attacks on September 11, 2001 occurred, he decided that USAA had to do more. "Sept. 11 forced us to raise the bar on ourselves," said Yates. [3]

Duffy continued the magazine article by describing what Steve Yates did to address the problems he found at USAA. Yates hired outside consultants, and along with measures to take care of the building and equipment that USAA needed to operate, he also set up a series of large scale business continuity and disaster recovery exercises. Yates wanted to learn how well the individual units within USAA would handle a major disruption of business wide activities. [3] In March of 2002, Yates started preparation for testing employees by simulating the loss of USAA's primary data center for its federal savings unit. In this exercise, the systems, applications and all 19 of the third party vendor connections were successfully recovered. More tests involving other business units were conducted in July and August. However, all of these tests only led up to what Yates considered to be the main event. The real test of business continuity not only involved the physical systems and the data contained therein, but also included the most unpredictable element in any business, its employees. Yates would find out just how much the employees could do on his main event, scheduled for July 24, 2002. [3]

Basic Principles to Follow

This example from USAA covered many of the principles and practices necessary to create and maintain a business continuity and disaster recovery plan for employees. Derek Slater of CSO magazine provides a list of basic ideas needed when creating this plan. [9] As mentioned above, business continuity and disaster planning are closely related. CSO magazine tells us that these plans need to include how employees will communicate, where they go during a disaster and how they will keep doing their jobs. CSO provides a list of the essential elements a business continuity and disaster recovery plan should cover:

- Develop and practice a contingency plan that includes a succession plan for your CEO.
- Train backup employees to perform emergency tasks. The employees you count on to lead in an emergency will not always be available.
- Determine offsite crisis meeting places and crisis communication plans for top executives. Practice crisis communication with employees, customers and the outside world.
- Invest in an alternate means of communication in case the phone networks go down.
- Make sure that all employees-as well as executives-are involved in the exercises so that they get practice in responding to an emergency.
- Make business continuity exercises realistic enough to tap into employees' emotions so that you can see how they'll react when the situation gets stressful.
- Form partnerships with local emergency response groups-firefighters, police and EMTs-to establish a good working relationship. Let them become familiar with your company and site.
- Evaluate your company's performance during each test, and work toward constant improvement. Continuity exercises should reveal weaknesses.
- Test your continuity plan regularly to reveal and accommodate changes. Technology, personnel and facilities are in a constant state of flux at any company. [9]

Lessons Learned

A casual reader may notice that each of these elements involves people, both inside and outside of the business. While it is true that testing a disaster recovery plan can be considered disruptive, how much more disruptive will it be when an actual disaster comes and employees do not know what to do? In the USAA example above, Steve Yates discovered that those employees who walked through the simulated disaster were in a better position to discover flaws in the business continuity and disaster recovery plan as well as offer advice on how to mitigate or eliminate those problems. [3] Yates also learned that those employees who had practiced for a disaster were much less likely to panic should that disaster materialize. CSO magazine also provides some discoveries made by other businesses in preparing and testing business continuity and disaster recover plans. Because there was a chance that employees could become trapped in their office building, one company started looking into stocking MREs (Meals Ready to Eat). Mike Hager, the former head of security at Oppenheimer Funds, discovered that few companies have provisions in their plans for alternate work places. Hager said that after the collapse of the World Trade Center on 9/11, there was only 10 million square feet of office space available in the whole of Manhattan. Even USAA, who arranged for alternate office space in a separate location, discovered that setting up the computers and other equipment took nearly two hours. This would be two hours that employees would be left out in the elements (in this case, USAA employees were left standing in the hot Texas sun for two hours). [3]

Tell It to the Boss

Lastly, the top executives might need some persuasion to implement the recommendations that are part of the business continuity and disaster recovery plan. Security managers and executives should stress the potential losses a company would face if the plan were not implemented and practiced. Work with legal and financial departments to document, day by day (and hour by hour if necessary), the losses that the company would suffer if it were paralyzed by a sudden (or expected) disaster. Explain to the top executives that business continuity and disaster recovery planning are another way of saying risk avoidance. A top executive would more likely respond to a plan if the security person can demonstrate how much risk they top executive would be taking if he or she didn't implement the plan. [9] More information for employee preparedness can be found at http://www.ready.gov/business/talk/index.html.

DISASTER PLANNING AND DATA

Forty years ago, the biggest threat to a company's data might have been a fire or a flood that would destroy all of the paperwork in their filing cabinets. Today, company data is increasingly entered, stored and processed on computers and other electronic equipment. This trend, unfortunately, brings with it a whole new group of problems and threats to plan for in the event of a business busting disaster. Some of these new problems include equipment failure, electrical power surges or outages, an inadequate or nonexistent data backup policy, fires, floods, lighting storms (it's still a threat, especially to electronics), mobile device security issues, malicious software, and malicious or incompetent employees (yes, it applies here, too). This section will cover basic data security, data backups, data security for mobile devices (including VPNs), and virtualization.

Basic Data Security

Basic data security starts with the user, but can be augmented by several sets of computer software programs. Anti-virus software will help to prevent malicious software such as viruses, trojans, and worms from infecting the network and spreading to every computer. Firewalls act as gatekeepers for people and programs, preventing unauthorized data from getting in (or out) of the company network. [2] Malicious software is another threat that all businesses face. Some examples include adware (advertising software), key loggers (what passwords have you been typing?), spyware (is your personal information at risk?), and even unwanted email (SPAM!). The Department of Homeland Security (DHS) provides some good advice on its website www.ready.gov. They recommend keeping anti-virus software updated, since new viruses and other threats are created constantly. DHS also advises people not to open email from unknown sources, or the attachments that come with them. DHS also informs us of two kinds of firewalls, hardware and software, that protect individual company computers as well as the network paths that connect them. [2] Another bit of advice from DHS is to use hard to guess passwords for logging into computers and computer services. This means that the password should not be something easily associated with the user (meaning it's easy to guess). The password should also be at least eight characters long ("gum" is not a secure password, nor is "Bill"), and contain a mix of numbers, special characters, and upper and lower case letters ("h8^&dn2p]" would be an effective password). DHS stresses that passwords should not be written down (too easy for others to find them), and that passwords should be changed frequently for the best security (it may be annoying to learn passwords, but it's better then getting fired for letting someone compromise the computer network). [2]

Caught with their Hand in the Honey Pot

Unfortunately, not everyone in the company will follow these basic guidelines, and even the upper management is not immune to error. Antony Savvas, a writer for Computer Weekly magazine, tells of how many top level managers and executives in the UK were duped into compromising their computers. [8] The NCC group, an IT security consulting service, conducted a campaign targeting more than 14,000 senior level decision makers in Bluechip companies (Bluechip means financially sound). By way of email and social media websites, NCC distributed a game called "Bish Bash Bush," a game about President Obama and Hillary Clinton kicking the former administration out of the White House. Not only did executives and managers open the email from an unknown source, they followed an unsecured link to an unknown website to play the game. NCC reported that senior staff at a third of these Bluechip companies fell for the trap. Not only did they play (during office hours), the senior staff members also forwarded the game's link to other employees in their companies. The article mentions that this game was now being played in 19 countries, including Azerbaijan, Chile and Bermuda. This only demonstrates how easy it is to dupe even the top brass in a company into ignoring basic security protocols. [7]

Data Backups

The next issue in preparing a business continuity and disaster recovery plan is data backups. For those who are not familiar with the word, it means that you take the information on the computer and copy it to something else in case that computer fails and the information on it is lost. All data that cannot be easily replaced should be backed up in case of hardware or software failure. Gennifer Biggs, a writer for Business Solutions magazine, provides some useful insights into this area of business continuity and disaster recovery planning. [1] Terian Solutions, a Houston based company, discovered that their current data backup plans were less than adequate should a disaster cause them to lose their data. Ron Pollvogt, the CTO (Chief Technology Officer) had several things to say about their aging system. He said “They knew they had problems with the reliability of their existing system, they knew their DR preparedness was not adequate, and they knew it was time to move beyond their legacy system [tape with some disk-to-disk].” [1] After conducting a discovery session within the company, Pollvogt learned that the reliability of the backed up data left much to be desired. Based on the logs that he reviewed, the failure rate for the backups ranged from 30% to 40%. To remedy this problem, Terian decided to replace the entire system with a completely new system that uses remote backup capabilities. To do this, Terian procured the services of Asigra Televaulting remote backup and archiving software. In the end, this change saved Terian $25,000 a year and has basically eliminated the failures that plagued the old system. In addition to these benefits, Terian implemented enhanced testing and reporting capabilities to further improve the reliability and accessibility of their backed up data. Having this system in place leaves one less thing to worry about in a business continuity and disaster recovery plan. [1]

Planning for Mobile Data Devices

Mobile devices such as laptops, smartphones, PDAs (Personal Digital Assistants) provide another major issue in developing and implementing and business continuity and disaster recovery plan. Because these devices routinely leave the more secure office area, they pose a much greater risk of having data stolen, lost or otherwise corrupted. It seems that every day, another major business or financial institution has had the personal information of its customers compromised because of a lost or stolen laptop. An effective method to mitigate this risk is to encrypt the disks where laptops store the data. In addition to the laptops, encryption can also be an effective tool in securing data and drives within the company building. David Strom, a writer for Baseline magazine, describes how the Prudential Financial Company implemented Vormetric's Data Security Expert encryption software. This software allow Prudential to selectively encrypt the most critical data at the company, and allow the servers to operate without being slowed down by whole disk encryption schemes. In addition to the extra security encryption provides, the Vormetric software will also scale as the Prudential Financial Company expands. [10] Having this system in place helps to prevent data loss disasters caused by malicious actions by people from within and without.

Other mobile devices, such as PDAs and Smart Phones, need to be included in the business continuity and disaster recovery plan. In Baseline magazine, David Strom covers methods where these devices can be effectively and securely. He mentions that hand held devices can be a very effective tool for data entry. Unfortunately, the wireless nature of these devices also means that security is several degrees harder to enforce. [10] To prevent unauthorized parties from stealing the data entered in these devices, Strom recounts what the Hill County Memorial Hospital did in Fredricksburg, Texas. The hospital used Treo smartphones to send patient data to and from hospital employees working in the field. The hospital's network administrator, Ira Babb, implemented VPN software created by NCP Engineering to securely pass the data to and from the Treo smartphones that were used during these home visits. [10]

VIRTUALIZATION

One more area that has been gaining ground in terms of business continuity and disaster recovery planning is the use of virtualization. In virtualization, different server functions (like web servers and databases) can be run from a single piece of hardware using virtual machines, saving on costs both in purchasing and in energy expenditure. This, of course, means that the hardware has to be quite powerful to run multiple servers on the same hardware, but technology has advanced sufficiently that this is now possible. Arif Mohamed, of Computer Weekly magazine, describes how the Royal London Asset Management Company deployed virtualization as part of their business continuity and disaster recovery plan. [4] The drive to virtualization actually started as an effort to cut costs and increase efficiency. As the company expanded, Dennis Leeks, the IT manager for the firm, realized that they were running out of physical space for their servers. On top of that, the heat produced by the company servers put a major strain on the building's air conditioning. When Leeks started consolidating servers with virtualization, he was able to save on space and electricity usage for both the computers and for cooling the room they were in. [4] In addition to this, because the servers were now virtual residing as a large file on a single server, backing up and restoring any or all of the servers became greatly simplified. The time necessary to recover from a disaster had been cut down to a matter of hours. One more bonus for the company, it was now possible to duplicate and test different configurations for each server residing on the machine. [4]

However, even in virtualization, there are risks. The biggest problem in using virtualization is the threat of intruders getting access to the software that controls the virtual machines. Jim Mortleman, of Computer Weekly Magazine, gives several tips in securing virtual machines. These are as follows:

- Appreciate the architectural differences of a virtual environment and adapt security policies accordingly.
- Ensure all virtual machines are fully patched and secured on an ongoing basis (including dormant ones), consider automated tools or managed services to ensure this happens.
- Apply intrusion detection and antivirus software to all physical and virtual layers
- Avoid ‘VM sprawl’, enforce policies to ensure VM creation is closely monitored and machines are decommissioned after use.
- Use secure templates for the creation of new VMs. [5]

DISASTER PLANNING AND EQUIPMENT

The last area of business continuity and disaster recovery planning includes not only the physical computer equipment, but also the buildings that those computers are housed in. Having a perfect policy with completely trained employees and perfectly hardened computers and servers will mean little if there is no power to the building, if the equipment is destroyed or stolen, or if the building itself is damaged or destroyed. This last section will cover physical access to business grounds and equipment, protecting and maintaining the infrastructure necessary to operate that equipment and what supplies will be needed for both preserving the equipment and the people that use them.

Locking it Down

Physical access is the first, most basic layer of security for any business. If a thief cannot get past the guard at the front door and the back door is securely locked, then chances are pretty good that nothing will be stolen. Unfortunately, as mentioned above, many of the problems come from the people already inside the building, the employees. Not only do the doors on the perimeter of the building need to be secured, but so too do the doors to server rooms, and any other areas that are critical to a business's well being. [6] The National Federation of Independent Business (NFIB) provides several guidelines in terms of physical security. One such guideline is to limit physical access. This applies to employees and non-employees alike. If an employee has no business being in a particular area of a building, then they should not have the keys or pass cards that grant access to that section. Some businesses have areas where they welcome customers and business partners. However, these same people should not be allowed in areas where they do not belong. The responsibility of watching for unauthorized access falls upon the entire staff, not just the security guard at the front door. [6]

Physical access also includes access to the computers, especially computers that can host removable storage (which is all of them). Referring back to David Strom's article in Baseline Magazine, a company needs some form of access control on its computers as an extra layer of security. Strom describes what Mammoth Hospital in Mammoth Lakes, California did to prevent someone with a USB drive from stealing patient data from an unattended computer. [10] Paul Fottler, the hospital's IT operations supervisor, installed software called

Device Lock on over 300 of the hospital computers. This software allows Fottler to lock down any removable access devices. This includes USB flash drives, CD and DVD drives, infra red ports and even Bluetooth access. Any port on the computer that can host a removable storage device can be locked down to prevent data theft. [10]

Providing a Good Environment

The next area to assess in equipment is ensuring that the computers and other electronics have an environment where they can function properly. The National Federation of Independent Business (NFIB) gives some pointers in this area as well:

- Develop an alternate power supply. Backup generation, which can keep your computer running for a short time period during a power outage, can help prevent data loss. If the cost of data reentry is high, backup power might be a cost-effective alternative. [6]
- Protect against power surges. Electrical storms can cause sudden power surges and spikes, or they can even occur randomly. The result? Lost data and, occasionally, damaged equipment. Good surge protectors cost little more than $100 and always make a wise investment. [6]
- When the air crackles, disconnect the modem. Electricity can easily travel through telephone lines during an electrical storm and can damage computer equipment through your modem. [6]
- Be sure you're insured. Your insurance policies should cover your hardware and software. Check with your agent. Data and records, however, are another matter. Just the same, ask about the availability and cost of critical records coverage. [6]
- Keep food and beverages away from your computer equipment. That means no sipping coffee while working at the keyboard. [6]
- Maintain the right temperature. While a dry, cool environment is best, most computer equipment can tolerate a wide range of temperature and humidity variations. But watch for excessively warm or damp rooms; they invariably spell trouble. [6]
- Clean your computer. A large proportion of system crashes occur because of dust and dirt. Have your CPU, keyboard and printer professionally cleaned on a regular basis. [6]
- Write down a plan. Your computer protection and security program should be just that—a program. Once you've developed concrete procedures to safeguard your data, write them down and either take on the responsibility of administering them or assign the task to a trusted employee. [6]
- Don't minimize the threat of a computer disaster by claiming "it can't happen to me." It can and probably will. Computers are machines and, even in the absence of earthquakes, hurricanes, floods, viruses and computer crime, machines can suddenly break down for inexplicable reasons. [6]

Supplies for Survival

The final area of business continuity and disaster recovery planning for equipment deals with supplies those employees will need to keep their equipment and themselves alive and well during any potential disaster. Much of this equipment is required by law, but others may not be included in that list. The Department of Homeland Security provides yet even more useful information on its website, www.ready.gov, in terms of what items an office building should have and what practices employees should remember. Some of the things that employees should be familiar with include: fire extinguishers, smoke detectors, building and site maps, emergency numbers, and routes for escaping the building during an emergency. Of course, if escape is not feasible, the employee might remember what one company did (see above with the MREs) and store adequate supplies of food and water to survive in the office if need be. No matter how well supplied a building may be, if the employees do not know what they have, or are not practiced in using those resources, they will not do well in the event of a disaster. [2]

CONCLUSIONS

Disaster Recovery is a constant issue in the business world. As long as businesses exist, there will be the threat of disaster, whether it stems from nature, from a malicious or incompetent employee, or even if the hardware just fails taking critical data with it. The most important part of business continuity and disaster recovery planning falls on the people. Without the people then the plan for protecting and preserving data and equipment become **meaningless**. There is more to business continuity and disaster planning than what is described in this paper.

However, any planning must be adapted the needs and resources of the business to which it is applied. The best business continuity and disaster recovery plan is the one that the business tailors to its own unique needs and people.

REFERENCES

1. Biggs, Gennifer. (2009, January). Use Off-Site Archiving to Improve Reliability. Business Solutions. Retrieved from http://www.bsminfo.com on February 28, 2009.

2. Department of Homeland Security. Read Business. Retrieved February 24, 2009 from the World Wide Web: http://www.ready.gov/business/index.html.

3. Duffy, Daintry. (2002, November 8). Building a Disaster Exercise Plan. CSO. Retrieved from http://www.csoonline.com on March 2, 2009.

4. Mohomed, Arif. (2009, February 27). Royal London Asset Management deploys VMWare. Computer Weekly. Retrieved from http://www.computerweekly.com on March 2, 2009.

5. Mortleman, Jim. (2009, February 27). The Virtualisation Threat. Computer Weekly. Retrieved from http://www.computerweekly.com on March 2, 2009.

6. NFIB. (2005, November 1). Data Disaster: Planning for a Computer Meltdown. National Federation of Independent Businesses. Retrieved from http://www.nfib.com on March 2, 2009.

7. Savvas, Antony. (2008, December 9). Top 10 Data Loss Disasters of 2008. Computer Weekly. Retrieved from http://www.computerweekly.com on March 2, 2009.References

8. Savvas, Antony. (2009, February 4). Third of senior staff at top firms fall for game honey trap. Computer Weekly. Retrieved from http://www.computerweekly.com on March 2, 2009.

9. Slater, Derek. Business Continuity and Disaster Recovery Planning: The Basics. Message posted to http://www.csoonline.com.

10. Strom, David. (2009, January 8). Assessing Your Endpoint Security Needs. Baseline. Retrieved from http://www.baselinemag.com on February 27, 2009.