Disaster Planning

An IT Perspective

By Jonathan Niebergall

Disaster Planning
An IT Perspective

A disaster is defined as an unforeseen, ruinous, and often sudden misfortune that happens either through some hostile external agency or through lack of foresight. On any given day you can turn on your television and learn about disasters that are occurring all over the world. These range from man-made to natural disasters. From a company standpoint, you must be prepared for any disaster. You must know how you will get your business up and running again as quickly as possible. Disaster recovery, in this regard, is the coordinated process of restoring systems, data, and infrastructure required to support key ongoing business operations.

For my Certified Insurance Wholesaler (CIW) project, I worked with Mollie Cipriano, our Human Resource Director, to put together the disaster recovery plan for R. W. Scobie, Inc. My discussion in this document will focus primarily on the project from an Information Technology (IT) perspective. As Team Leader for the IT Department at R. W. Scobie, I was responsible for making sure that safeguards were in place to deal with any disaster. I also had to make sure that any IT issues were taken into consideration in the disaster recovery plan document. I will primarily discuss information on system issues that I needed to research before putting a disaster recovery plan in place. Then, I will give an overview of what I found out in putting the plan together and how and why IT needs to be involved in the actual disaster plan document for any organization. (A copy of the R. W. Scobie Inc. disaster recovery plan is included at the end of this document.)

In looking at a disaster recover plan from an IT standpoint, it is necessary to be proactive and not reactive. Nearly 80 percent of U.S. companies do not have sufficient plans and solutions in place to address network outages or system failures that could interrupt the flow of business information. While many businesses have data back-up systems, very few have a plan to access that data if and when a disaster occurs.

Statistics were reported in a survey conducted by SunGard Availability Systems. The survey, which polled 200 U.S. businesses with $5 million or more in annual revenue in a broad range of industries, was conducted by New York research firm David Michaelson & Company, LLC. According to the survey, small companies are not in good shape when it comes to disaster preparedness. Thirty-nine percent of small companies are less likely to have written plans in place. Of those polled, only half of those with a plan had tested it in the past six months. Twenty percent of those with a plan have never conducted testing.

From a technology standpoint, there are internal and external threats that you need to be aware of and take care to protect yourself from. Internal security is the process of securing your network from internal threats, which are generally much more common (greater than 75 percent) than external threats. Examples of internal threats include:

- Internal users inappropriately accessing information to which they should not have access, such as payroll and accounting records.
- Internal users accessing other users' files to which they should not have access.
- Internal users impersonating other users and causing mischief, such as sending e-mails under another person's name.
- Internal users compromising the security of the network, such as by accidentally (or deliberately) introducing viruses to the network.
- Internal users "sniffing" packets on the network to discover user accounts and passwords.

External security is the process of securing the network from external threats. Four basic types of external security threats exist:

- Front-door threats – these come from someone outside the company who is able to gain access to a user account. The most common among this type is the disgruntled or terminated employee who once had access to the network.
- Back-door threats – these are often directed at problems in the Network Operating System itself or at some other point in the network infrastructure, such as its routers. The best way to prevent these problems is to stay current with your NOS software and any security-related patches that are released. Web servers are a frequent target for hackers.
- Denial of Service threats – these deny service to a network resource to legitimate users. These often target e-mail and web servers but can affect an entire network. DoS attacks usually take one of two forms: they either deny service by flooding the network with useless traffic, or they take advantage of bugs in the network software that can be used to crash servers. To help prevent DoS attacks, make sure to keep your various network software current. Also, use settings on your firewall to control traffic into the network and deny access to servers from outside the LAN that do not need to be accessed.
- Viruses and other malicious software threats – these threats would include :
    - Viruses – a program that spreads by infecting other files with a copy of itself. There are 30,000 + known viruses in existence today with more being written and discovered daily.
    - Worms – a program that propagates by sending copies of itself to other computers, which in turn run the worm and then send copies to more computers. These have spread through e-mail systems like wildfire lately.
    - Trojan horses – a program that purports to do something interesting or useful and then performs malicious actions in the background while the user is interacting with the main program.
    - Logic bombs – malicious pieces of programming code inserted into an otherwise normal program. They are often included by the program's original author or by someone who participated in developing the source code. Logic bombs can be timed to execute at a certain time, erasing key files or performing other actions.

From an IT perspective, to protect a network from virus attacks you need to implement some type of antivirus software. Antivirus software runs on computers and the network and "watches" for known viruses or virus-like activity. The antivirus software then removes the virus leaving the original file intact, quarantines the file so it can be checked by an administrator, or locks access to the file in some other fashion. Rely on desktop software only as a back-up to running server-based software, because employees can and will disable such software on occasions.

Once you are aware of what kinds of disasters can happen, you can focus on protecting your system before a disaster occurs. You need to address main technical areas including: hardware, networking issues, software, and data.

Hardware issues include machine type, configuration (disk capacity, peripheral devices, device names, RAM, file systems and volume groups, OS users, etc.) and operating system version and patch level. Another issue to consider during a disaster is whether to use an existing preconfigured machine or to completely configure a new machine (load the OS, initialize and configure disks, TCP/IP configuration, SCSI addresses, etc.). An option may be to keep computers that you upgrade as back-ups stored at another location off-premises. If you need your old machines in the future, they might seem outmoded and slow, but you will still be able to use them to get you up and running. One suggestion was to keep enough of your old computers to replace 10-15% of your working computers.

Another suggestion is to keep spare server hardware available. Servers are constantly working, and parts tend to wear out. One of the components that commonly fails is a network card. It is recommended, if you have a free slot in the server, that you install a spare card and then disable it. If you need it, it will only take a couple of minutes to switch over. You should at least have another card on hand which is identical to the one that is in your server. Many of the new servers come installed with spare power supplies, but this is another component that is known to commonly fail and should be kept on hand. A step up from having spare parts on hand is to have a spare server available. This is the option that is used by our office. We have a spare server located 100 miles away from the office that is available in case our main server is not functioning.

When dealing with networking issues there are several questions that will need to be answered to best handle your individual situation. These include:

- Is any special type of LAN or VPN software required?
- How do the machines communicate with one another (probably TCP/IP)?
- Do applications connect to machines using hostnames or hard-coded IP Addresses?
- What other configuration information is required?
- Are there requirements for connections to an external network (WAN, Internet, Extranet)?
- Are there requirements for dial-in access?
- Is there any other type of Client/Server activity that will need to be supported?

All networking requirements and issues need to be identified, documented, and then addressed in the disaster recovery plan.

Dealing with software issues is a very broad area. This may encompass many different things including the Operating System, user written applications, and third party software. A comprehensive inventory of currently used software, including current versions, license information, and support contact information are essential to record in your disaster recovery plan. You should also make copies of your software programs on CD-ROM and store them offsite. The computers you use to replace your destroyed computers will be useless without the software you need to run your operation. You should also have any installation media, installation guide/notes, and current configuration settings documented, as you cannot guarantee that your systems administrator will be the one trying to set up these new computers.

Data is a vital asset to businesses of all sizes, so it is crucial it be protected at all times. One of the most important aspects of a disaster recovery plan is to decide how and where you will back up your vital data. You first must decide on the media to back-up your data. There are many different types of media that you can use for your back up. Several of these are: ZIP drives, CD-ROM/RW, DAT DDS-1 & 2 drives, Digital Linear Tape and removable hard drives. We have recently changed over to the removable hard drives with our new server. Whatever media you choose, you should clean your drives periodically. This can be done by your IT staff, but having an authorized maintenance person from the manufacturer or a third-party repair firm check the equipment every 12 to 18 months is something to consider.

Proper storage of back-up media is a crucial aspect to your back-up process. You will probably keep most of your back-up media on site, so you need to provide a location that is stable without extreme temperature, humidity or electromagnetism. It is not wise to store your media on the other side of a wall from a large generator whose electrical fields can wreck havoc with the data on them. Off-site storage is a must for at least your most current back-up, if not for your last two. This can be accomplished by having your IT administrator, or another employee, take the back-up home at night. Another option is using an off-site storage firm that provides fire-protected storage facilities for digital media as well as tape.

A new option for data back-up that has emerged is an Internet based real-time back-up system. Here, the public Internet is used to build an offsite disaster recovery system. This type of system provides encrypted data transmission between local and remote sites with real-time data back-up at a lower cost then previously used dedicated communication lines. This is an option that we have incorporated into our back-up process to supplement our daily system back-up. We transmit data between our main server located in the home office with another server located in a remote office 100 miles away. This is done every 30 minutes.

Now that the systems were protected and backed-up, I found that I could focus on the actual disaster recovery plan document. It was much to my surprise, that when I sat down to put the document together, how much the IT department still needed to be involved in the planning. The IT department's role did not end with the network protection and back-up. Not only did we have to plan for setting up our systems and restoring our data, but I found that we would be working with almost all other sections of the disaster plan.

The disaster recovery plan that we put together started with a Recovery Team that was made up of decision leaders in our company. Each of these leaders was responsible for coordinating of a section of the plan. I took the role of the IT coordinator. In this position, I took the knowledge from the research that I had done and put it in place in our office. This also included putting together a key IT supplier call list. I had two responsibilities in this role during a disaster. I had to be responsible for acquiring replacement equipment, if needed, and to restore all software and data as soon as possible following a business interruption. For our plan, we decided that there was a 72 hour window to be up and running again. This seemed pretty straight forward, but what I found out, as we started putting the other sections of the disaster recovery plan together, was that I needed to work closely with those coordinators.

When looking at the internal and external communication sections, it was required that we have a list of all agents and companies that we did business with. This was information that we would have to extract from our database and put in a format that we could transfer to a third party for mass notification at time of a disaster. We also had issues with phone systems being available, which I found to be another technology issue that needed to be addressed. I have not explored this issue in this paper as I have not worked closely in this area, and we have contracted with an outside vender to work with us on telecommunication issues.

Two other sections of our disaster recovery plan that I became involved in were the move and alternate location sections. Once we started talking about purchasing new equipment, we had to plan on moving all this equipment also. Getting 50 to 100 new computers and monitors to an alternate location may present some problems.

The location that we were going to relocate to had to have specific requirements in regards to phone and internet access. This was something that had to be researched to determine who could handle our needs. It was pretty easy to find a hotel or local convention center that could handle us for a short amount of time, up to one week, but what if we needed a more permanent location? If our building had to be partially rebuilt and we needed to relocate for six months or longer, what would we do then? We were able to find a business that had space we could use in case of a disaster. There are "hot sites" available in some areas that might also be an option. This area will need to be reviewed frequently as new locations become available or for some reason an alternate location becomes unavailable. It is highly recommended that an agreement be drawn up between both companies to protect each other.

The last coordinator I found that I was going to have to work with was the salvage and security coordinator. Once they determined that it was safe to re-enter our building, it would be up to the IT staff to evaluate all our equipment to see if some could be moved to a new location or had to be replaced. We would need to complete inventory checklists of what was still usable and was taken out of the building. We would also have to work with a local vender that dealt with recycling of computer hardware for the destroyed equipment. This is something that we don't want them just hauling off to the local dump as equipment needs to be cataloged and hard drives need to be erased.

When I first looked at doing a disaster recovery plan for my CIW designation, I thought that I had a strong knowledge of what would need to take place from an IT standpoint. What I found out was that there was much research to do before actually sitting down to write the document. I found that no situation will be the same for any company as different hardware, software and network systems are used. Each company must look at what is available and decide what works best for them based on needs and cost. There was also the shifting of a paradigm that disasters didn't have to come with 120 mph winds, but could be caused by the stroke of a key on a keyboard. Whatever is put in place by a company in regards to a disaster recovery plan, the greatest error that anyone can make is to leave that plan on the shelf and never look at it again. It is a document that needs to be reviewed at least annually if not more frequently for certain areas. Technology is always changing and new solutions are always presenting themselves.