More on Disaster Recovery

In my last post on Disaster recovery, I discussed that backups can lead to a false sense of security and that the only thing that really matters is the ability to restore. This is still absolutely correct. In some circles it is a new and controversial idea; most experienced IT hands immediately recognize the need to restore as an absolute truth. Today I want to discuss some other elements of disaster recovery planning - there is much more to it than just getting restorable backups. Here are some additional vital points:

Managing Staff:

Depending upon the nature of the disaster and your company's response to the disaster, managing staff can be the most important and potentially impactful of all tasks. Why? Very simple. *People* respond to disasters not computers. It takes the flexibility and judgment of human intelligence to respond to these situations. No matter the level of preparedness you may have, organizations are in a constant state of flux. The environment your organization is operating in is in a constant state of flux. What makes this even harder is the impossibility of predicting every detail of what is going to happen and people's responses to the situation. Some examples are in order.

Assume for a moment that your group was smart enough to have offsite storage of your data and software. Good to go right? Maybe not. Perhaps there is an unexpected human factors event that interferes with access to the physical site where your backups are stored. Perhaps, the union that normally transports the secure backups goes on strike and suddenly you cannot get the normal transport and access to your backups. This means you may have to send staff out of town to pick them up directly from the vendor. This also engenders several corollary factors. Transport of your staff (and associated costs), willingness of your staff to cross the picket lines, perhaps police escort, impact of news media coverage, etc.

What about non-human factors? To be blunt, mother nature could not care less that there was a hurricane that destroyed your datacenter. The two bridges that connect to the main roads to reach your data are currently impassible. What now? It all depends. Is it worth the cost of a helicopter rental to take an employee from an access point into the premises where your backups are stored? Only you and your management can judge the relative cost effectiveness of getting your data and software back a few days sooner. Certainly, some measures of cost should already be in place to help make this decision, but it is still a judgment call. This not something ChatGPT can easily answer. Human judgment is a critical component.

A different but still very pertinent example is physical access. In the event of a fire or some other incident, there are normally areas that are off limits to the public. The critical employee who knows which servers to try to pull from the ashes of the building or exactly where the data

safe is in the wreckage, has to be able to get into the disaster scene, has to know how to behave when dealing with the civil authorities, has to know how to deal with the insurance agents and inspectors and all the rest.

The same employees have to be known to the insurance companies and the local authorities must be made aware that Susan and Tom are coming with a U-Haul truck to take certain items and they have special authorization to take certain items from the scene. A company ID badge is often simply not enough to get access into a space that is being supervised by government authorities. You may find your erstwhile employees under arrest if they just show up and start messing around inside a burned out building without prior arrangement with the police and the insurance company. I have been in buildings where certain secure materials were held that, if you crossed the red line, the SEALS might try to ask you what the heck you thought you were doing there, that is, assuming you are still alive after some of the world's best marksmen have shot you. I am completely serious about this.

Another element of this is the actual or potential toxicity of the environment. When some things burn, they give off toxic gases that can concentrate in certain areas. Or if Uninterruptable Power Supplies were in place, they might hold residual energy that no one is expecting. The place may be full of water, which can be a pretty good conductor. The whole point is staff should be specifically trained to go into hazardous areas if you ask them to. It is important that people know what to touch and what not to touch. They need to know when to wear the appropriate protective gear. The biggest problem is what is safe and what is not safe is not always obvious.

It might be very appropriate to hire a company that specializes in recovery of materials from damaged facilities before proceeding. This brings us to another topic, a topic which is almost always vital to getting things done in the world. Money.

During a disaster situation physical money and general funding can be surprisingly difficult to access. Depending upon the type and scope of the disaster, ATMs may not be functional, and Electronic Funds Transfer activities may be suspended. In essence, sources of funds may suddenly dry up.

There are several actions an organization can and should take place in advance of a disaster to ensure their ability to respond. Among these are:

1. Disaster recovery insurance – it should meet the approval by the IT director as well as financial managers.
2. If a company knows a disaster may be coming, they may decide to create relationships with financial institutions that are not locally based – the disaster preparedness of an organization's financial partner should be part of any evaluation of a potential financial partner.
3. Buy a certain amount of computer resources in advance of their need and fully stage them before the disaster occurs

4. One or more “Fail Over” sites where complete operations can be transferred at the press of a button.

The problem with all of these strategies is that they require considerable investment. There is no hard fast rule that can say exactly which method(s) a company should use. It takes analysis and thought of company’s financial position, its dependence upon IT resources, its customer base and how it exchanges with customers. This analysis takes time, research, attention to detail and imagination along with plenty of realism in estimation of effort and availability of resources.

The Auditors are Coming:

I have managed several disaster recovery plan creation efforts where a consulting engagement started with a somewhat urgent phone call from an IT Director where the main points were something like this:

1. We are a publicly traded company
2. Auditors will be here in a month (or less)
3. Our disaster recovery plan is, (I am thinking, oh no NOT AGAIN) as I listen to the IT Director describe the plan’s many inadequacies.
4. Please come, right away; I have authorization to spend money to get this done in a hurry as our stock price will take a hit if the auditor’s see how bad it is. They almost never say these exact words but it pretty obvious to a person who has some business understanding.

So, we move heaven and earth and make staff available and get started on the plan. Do the research, etc., etc. - all is coming along well. Auditors come, plan is not finished yet but significant strides have been made toward creating the plan, so the auditors write a small note that the plan is in progress and should be finished soon. Stock value disaster averted. The very next day I get a phone call from the IT Director of the client company that says: "*Good job, crisis averted. Take your people and go home*." But the plan is not finished, I say. IT-Director says – "*Oh we’ll get around to it. For now, I have to stop spending money. Don’t worry we will give you a good recommendation – you guys did great work. Bye!*"

What kind of nonsense is this you ask? I asked the same exact question to my VP when I told him we were sent home. To my shock he was not surprised nor angry. I thought I was going to be in trouble, as normally when you are “sent home” from a consulting engagement without a finished product it means you have messed up big time. Instead, my VP laughed and said, “Don’t worry this happens all the time.” I was flabbergasted!

Being the sincere innocent guy I am, I said,” But they kicked us out and their plan is more of a shell than a fully featured workable disaster recovery plan! Shouldn’t I call the auditors and raise the alert that they were being scammed?”

He saw the look on my face and continued," Welcome to the real world of business. We delivered well what they needed and wanted – a way to keep the auditors happy. If you call the auditor's and tell them that their work was shoddy and they were hoodwinked this is what will happen:

1. Someone will have to tell someone in internal management of the auditing firm (if they have the guts) that they messed up and much money and many man hours will have to be burned to clean up the mess. The clean up itself will be internally very difficult for the auditing firm.
2. It will get back to the IT-Director that we have created problems for him and his firm that they will now have to spend a substantial amount of money to fix.
3. The IT-Director will probably never engage us in another effort – thereby destroying a repeat customer.
4. The IT-Director will probably bad mouth us to other executives he or she knows thereby destroying many future opportunities for us.

In the real world you have done a good job. The IT-Director now has at least the outline of a workable plan, they may indeed get it finished with their own staff and they are much better off than they were before the engagement. Take your success and run with it!"

Practice Makes Perfect:

A disaster recovery plan gathering dust on the shelf may be better than none at all. Disaster recovery plans need to be practiced for many reasons. Three key reasons are:

1. Staff familiarity. People need to understand their roles and how to do them. They need to be trained on where they can go, what they can and should do as well as what they should not do.
2. Testing reveals flaws and ways to optimize the plan. Things change over time. In fact, the one thing you can guarantee is that things will change. Testing can reveal the little details. Mary was supposed to be given access to building Y in case of disaster but no one remembered to let the Security Department know, thus she could not get in the building to recover certain needed backup tapes. Testing can reveal how an evolving environment impacts the usability of your disaster recovery plan.
3. Executive visibility. When one and two above are accomplished, it is fairly easy to do a status report for an executive that outlines what went well, what did not go so well and make recommendations for enhancements. Remember, a good plan INCLUDES financial resources as well as technical resources and technology itself. Part of the testing should include a call from the company Treasurer to the bank who is supplying the funds or whatever the sources of funds may be. Financial markets change too. Perhaps what was a good financial partner for a disaster can no longer fulfill that role because lending requirements have changed. Financial markets can be volatile and this can impact

availability of funds to accomplish the plan. The point is the plan needs to be tested from end to end, including the business aspects of the plan.

Summary of this Post:

Reflect upon the factors I have mentioned above. An important, often neglected area of disaster recovering planning is how staff are applied in its execution. This is much broader topic then it might look at first glance. It includes safety of personnel, access to the building and a lot of liaisons with your disaster recovery partners such as senior financial management, insurance companies, local municipal authorities, etc.

1. To do it effectively takes financial resources. Planning for these resources in advance should be a mandatory part of the plan. Yet it is often forgotten or ignored because it takes commitment on the part of executives to be ready for the disaster that is going to eventually happen. A very small business can do simple, relatively inexpensive things, like making backups of data and programs and keeping them off-site. Even this requires some investment of time and money.

2. The real world is often far from ideal. Your job is to make it better. How much better you can make it is relative the willingness and resources available. Do not be disappointed that you were not able to create a perfect solution. What is truly important is that the situation is better and that you made people think about it and consider their options in advance. That alone is a major improvement and is a success of some magnitude.

3. The realities of business life are definitely NOT the ideal you may have learned in an educational institution.

This is probably more than enough for this particular post. Future posts will cover many more topics. One that seems to be of immediate importance is disaster recovery and "The Cloud"/Internet. Once again there is more to this than may be obvious. The Internet offers many services and options to provide information processing capabilities. It is very interesting how this correlates with disaster recovery. Some see it as a panacea and it certainly can be helpful. There are many different types of services available. We will walk through this particular garden\mine field in the next post.

Until then,

Happy Computing and may your backups always restore without issue!

Mark Massey

MCSE, MCP ID #316