

‘Mitigation’ The First Pillar of a Disaster Recovery Plan

By Rex Bullard

To think that a "disaster" will never happen to your organization is more than naïve - it's irresponsible.

Having a backup strategy, doing backups everyday and running anti-virus software does not mean you have a Disaster Recovery Plan.

According to the American Red Cross, 40% of small businesses that suffer a disaster will never re-open for business.



Before a Disaster Recovery Plan can be started an in-depth **Operational Analysis** should be undertaken.

The following areas should be reviewed as a minimum:

Physical Security

How easy is it for staff to obtain access to the physical servers? Can a determined person easily remove any server from your premises? Are your servers openly available to all staff and passers by?

The following is a list of questions you may consider asking when reviewing physical security.

- Are the servers located in a secure locked area with access limited to selected personnel?
- Are the servers locked when no one is around?
- Does the area around the servers have either a smoke or heat detector in place?
- Is the air conditioning adequate?
- Are the servers safe from external elements, like excessive sunshine, wind, dust and extreme hot or cold temperatures?

Vulnerability Assessment / Network Security



This is often overlooked as part of the disaster recovery process. There is a global database, available on the Internet, of known system vulnerabilities. An intruder can identify weaknesses in your network, simply by identifying what equipment you have running and what operating systems you are using. Is your network secure from outside intrusion?

- Does your company have a written security policy, including specific incident response procedures?
- Are steps taken to keep the procedures up to date?
- Is an adequate intrusion detection system (firewall) installed?
- Are procedures in place to communicate intrusions to the appropriate people?
- Are your IT support people trained on the specific security equipment being used?
- Does someone audit firewall activity on a regular basis?
- What are your vulnerabilities?
- What is at risk as a result of your vulnerabilities?
- What must be done to eliminate the vulnerabilities?

Critical Services

Review the current services that are essential to the daily operation of your business.

- More and more business is being done through the Internet. Something as simple as losing connectivity could interrupt critical services. What type of connectivity is in place? Do you need a redundant service?
- Does your business have adequate power protection? Is the Uninterrupted Power Supply (UPS) capable of protecting all your servers and for how long will the servers stay available in the event of a power failure?
- Do you need a back up generator?
- Phone services should be reviewed as well. Interestingly enough, phones are often overlooked by organizations that implement a disaster recovery plan. But what business could live without their phones for any significant period of time?

Passwords / User Accounts

Each company should have a written security policy that discusses how passwords should be managed.

- Does company policy require unique accounts (no 'guest' accounts)?
- Are users required to change their password on a regular basis (30-60 days)?
- Does the policy prevent users from reusing previous passwords?
- Are requirements in place that force the password to contain a combination of numbers and letters? Note: You may also want to avoid using common dictionary-based words in passwords as password crackers tend to look for these first.
- Does IT change server or main systems passwords on a regular basis?
- Have all generic user accounts, such as ADMIN, ROOT or HOST been disabled?

User accounts should be created with a standard methodology and naming convention. This should be included in the Corporate Data Security Policy. The policy should also encourage users to not share their passwords with other users, including their boss.

Backups / Data Storage



Many organizations make the common mistake that having a backup strategy in place is the same as having a disaster recovery plan. Doing backups on a daily basis is obviously encouraged, but that alone does not constitute a disaster recovery plan. The Operational Analysis should review the current backup strategy of the organization to make sure an adequate backup of critical information is being done. Key questions here include:

- Are backups done daily?
- Are backups kept offsite on a regular basis?
- Is there at least a two week rotation of tapes?
- Given the offsite storage practice, if there was a fire in your building, what is the potential exposure that your company faces with regard to lost data?
- Is that exposure acceptable?
- When was the last time a test was done to ensure that the data can be restored effectively?
- Are logs of backups kept and reviewed regularly?
- Is data stored at the workstation level that is not getting backed up on a regular basis?
- Does your company rely on users to back up their own data?

Internet Use and E-mail

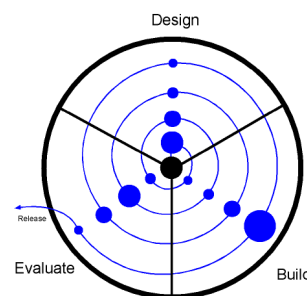
Do you have policies in place that restrict or monitor employee's usage of the Internet and E-mail. This is likely to be the area most likely to cause a virus to access the network. The Operational Analysis should review logs of user's access to the Internet and the need for corporate monitoring software. Do you require content filtering software to restrict access to inappropriate sites. Should you restrict e-mail attachments by size or type?

Anti-virus

The second half of the "poor man's" Disaster Recovery Plan is anti-virus software. Anti-virus software is a necessary tool, but even more necessary is a solid method of deployment to keep the environment safe. The Operational Analysis should evaluate what anti-virus software is being used at the workstation and server level. Determine what e-mail anti-virus software is in place. Also, it is necessary to determine what the procedures are for updating the software to keep it current. Having anti-virus software that is not current can be more dangerous to the organization than not having it at all. When the software is in place, we assume it is doing the job adequately. New worms or viruses are not detected by out of data software and will infect your system.

Documentation Review

One of the phases of the Disaster Recovery Plan is to document key systems and applications. Determine what documentation exists and how accurate and up to date it is. Identify any gaps and be prepared to document the missing pieces later in the project.



Network Review

Often a company will start with a basic network configuration, then add equipment to the network as their needs dictate. When this happens, it is difficult to maintain an accurate view of the network. Sometimes, we think that certain pieces of the network are securely behind the firewall, but by doing a review we may learn differently.

By having an independent review of the network, assumptions are bypassed and a clear view of the network is reported. Reviewing the network in this way provides you with a) a clear picture of the configuration, exposing any possible security vulnerabilities and b) documentation of the network configuration, which can then be valuable in the event of a disaster.

Penetration Testing

Some security conscious organizations may want to go as far as to hire a firm to perform penetration testing on your network. This takes the vulnerability assessment to a new level and not only shows what vulnerabilities exist, but demonstrates what parts of the network are open to attack. Only qualified penetration testers should perform this test.

Report

A summary of all of the information gathered during the Operational Analysis should be put together and be made part of the overall Disaster Recovery Plan. This documents the condition of the network at the beginning of the project. As areas of concern are uncovered throughout the review, action items or recommendations should be documented in the report. A checklist can then be made to monitor the progress of making improvements against the overall plan.

If you would like assistance to complete your Operational Analysis prior to starting your Disaster Recovery plan don't hesitate to contact **the sales team on 04 494 9670**

References:

Hoffman, Mark. "Designing a Disaster Recovery Strategy." *Info-Tech Research Group*. Info-Tech Research Group, 3 Sept. 2002. Web. 9 Oct. 2009. <<http://www.infotech.com>>.