10 Disaster Planning Essentials For Your IT Department

by Michael Moran, Affiliated
www.aresgrp.com

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

For more than 20 years, we have been involved in assisting many of our customers with creating and implementing disaster recovery plans, along with general recovery outlines, ensuring that they can minimize the downtime experienced in the event of a systems loss.

Our clients range from traditional industrial and supply chain companies, to professional and financial services organizations, non-profits, and even two technology-consulting companies. While every one of these organizations takes a slightly different approach to their planning and processes, they do share a great deal of common objectives when it comes to preventing and restoring their systems in the event a disaster occurs.

A "disaster" is generally defined as "a sudden calamitous event" or a "great misfortune or failure" and can present itself in numerous ways and on multiple levels. A broken device that cuts off access for some or all company staff may be considered a disaster to some organizations, where another organization may find a damaged pipe flooding a basement server room to be a disaster. Identifying potential disasters, and how to recover from them, are key to an organization's lifeblood.

Building a thorough Disaster Recovery Plan does take time; however, it becomes an invaluable asset, should your organization be faced with the unfortunate experience of a disaster.

Having built a number of plans, and having been involved in a variety of extraordinary events (from that broken pipe above the basement, to a major malware attack, a backhoe that pulled out an internet connection, a bad set of core switches and patch panels, to destruction of a corporate data center by a disgruntled employee), we know the value of having an updated plan, and the security it can provide to your organization.

Consider the impact to your bottom line: For an organization with $50 million in annual revenue, up to $250,000 of that is at risk for *each day* of downtime. This does not cover the company's fixed costs, payroll expenses, or recovery costs – so every hour of reduced downtime is extremely valuable.

This report is a summary of the knowledge we've gained resulting from experiences with disasters. It provides you with some guidance as you think about your organization, and your readiness to respond to an unplanned outage or disastrous event.

If you would like some assistance with your plan, or any of your IT needs, please refer to the offer at the end of this report. Simply contact us, and we will be happy to schedule a call or meeting to discuss your interests or concerns.

We welcome the opportunity to help you achieve your business goals,

Mike

Mike Moran

President, Affiliated

10 Disaster Planning Essentials For Your IT Department

If your data is important to your business, and you cannot afford to have your operations halted for days – even weeks – due to data loss or corruption, then you need to read this report and act on its information. A disaster can happen at any time, on any day, and is likely to occur at the most inconvenient time. If you aren't already prepared, you run the risk of having a disaster present itself before you have a plan in place to handle it. This report will outline 10 things you should have established, to make sure your business can be back up and running again in the event of a disaster.

1. **Have a written plan.** As simple as it may sound, just thinking through, in ADVANCE, what needs to happen if your systems have a meltdown, or a natural disaster wipes out your systems or even your entire office, will go a long way toward getting it back up quickly. At a minimum, the plan should contain details on what potential disaster(s) could occur, and a step-by-step process of what to do, who should do it, and how it should be done. **Once written, print out a copy and store it in a fireproof safe, have an offsite copy (possibly stored in the cloud), and file a copy with your IT consultant; then, update it at least annually.**
   a. **Outline the steps for the process of "restoring the system".** Have both a general outline and a detailed plan written, so that a "reasonable" IT resource can step in and follow your process.
   b. **Prioritize what needs to be restored and when.** Work with leadership to determine what applications or systems (phone system, network, wifi, etc.) must be back up and running, and in what priority. For example, if you can't afford to have your e-mail, website, or other "key" applications down for more than a few hours, then you need a plan that can get you back up and running within that required timeframe.
   c. **Include your documentation.** Include the network documentation (detailed in step 5) to ensure that you know what you have, where it is, and how it can be serviced, or replaced, quickly and in an orderly manner.
   d. **Include a communication execution plan for staff, key customers, and vendors (as appropriate).** Execute your commination plan (explained in step 2) to inform and update your staff, along with key outside resources, so that everyone understands the situation, knows the restoration schedule, and can perform their responsibilities accordingly, while the IT team works on restoring the systems.
   e. **Anticipate the unexpected.** As a part of the plan, consider what unexpected items/events might occur (your internal IT staff becomes unavailable, access is restricted, etc.) and consider your alternatives to ensure systems can still be restored in an orderly, timely fashion.

f. **Update the plan on a scheduled timeline –** then review the timeline with leadership to ensure the updates occur. New equipment, new/updated applications, additional facilities, all require that the plan is updated and accounts for the changes so that if an event occurs, nothing is "missing" that delays an effective restoration.

2. **Develop a communication plan.** If something should happen where employees couldn't access your office, e-mail, or use the phones, how should they communicate with you? Make sure your plan includes this information and incorporates MULTIPLE communications methods.

    a. **General Staff Communication-** Have a list with contact information for all staff members (not just e-mails or extensions), so that if an emergency strikes, they can be notified of the event and be advised as to what is expected of them. A call down list, or group text, could be used to provide the necessary communications.

    b. **Management/Staff Status Updates-** Agree on both a format and delivery vehicle for Status Updates (e.g. every 2 hours, every 4 hours etc.), so that key resources are aware of the status, and the IT team can be allowed to focus on restoration efforts.

    c. **Customer and Vendor Communications –** Based on the event, determine if/what messages need to be sent to key outside resources, and how those messages will be conveyed. Website, phone, e-mail communication disruptions can potentially be addressed with system messages, though personal contact may be needed for other contacts. Having a plan with responsible resources provides a consistent, smooth approach to business during a trying time.

3. **Backups – having access to your systems and data are key to recovery in the event of a system failure or physical disaster. Key areas of focus are:**

    a. **Automate your backups.** If backing up your data depends on a human being doing something, it's flawed. The #1 cause of data loss is human error (people not swapping out tapes properly, someone not setting up the backup to run properly, etc.). ALWAYS automate your backups so they run like clockwork.

    b. **Have an offsite backup, preferably digitally stored, of your data.** Always, always, always maintain a recent copy of your data off site, on a different server, or on a storage device. Onsite backups are good, but they won't help you if they get stolen, flooded, burned, or hacked along with your server.

c. **Image your server(s), desktops, and key network devices.** Having a copy of your data offsite is preferred, but also keep in mind that all that information will need to be RESTORED someplace to be of any use. If you don't have all the software disks and licenses, it could take days to reinstate your applications (like Microsoft Office, your database, accounting software, etc.), even though your data may be readily available. Imaging your gear is essentially making an exact replica; that replica can then be directly copied to another server, saving an enormous amount of time and money in getting your network back up. If you save a base image of your workstations, you will be able to reload them faster and easier. While your users may lose their preferences or favorites, they can still access their base systems and applications much faster than if you are required to manually reload each device. To find out more about these recommendation options, ask your IT professional.

4. **Have remote access and management of your network.** Not only will this allow you and your staff to keep working if you can't go into your office, but you may be able to start addressing an orderly recovery faster, especially if access to the physical location is blocked. Plus, your IT staff, or an IT consultant, should be able to access your network remotely, whether it is in the event of an emergency, or for general routine maintenance. Make sure they can.

5. **Network documentation.** Network documentation is simply a blueprint of the software, data, systems, and hardware you have in your company's network. Your IT manager, or IT consultant, should put this together for you. This will make the job of restoring your network faster, easier, AND cheaper. It also speeds up the process of everyday repairs to your network, since the technicians don't have to spend time figuring out where things are located and how they are configured. Finally, should disaster strike, you have documentation for insurance claims of exactly what you lost. Again, have your IT professional create this documentation and keep a printed copy with your disaster recovery plan.

    a. **Network Diagram** – Create a network diagram identifying all the devices (and their locations) on your network. Having IP addresses and other asset identification will help everyone see the layout of the company network.

    b. **Rack or Server Room Documentation** – Build a graphic of each rack with items listed (again, include asset information) and identify the device use or applications hosted (if you use a server or IT room without a rack, create a similar graphic so resources can easily identify each device). Having this will assist in the event of a "physical disaster", and help you and your team know what device is located where and its purpose.

c. **Asset Inventory** – Compile a list of the organization's IT assets; include device, manufacturer, model SSN, base configuration, age, maintenance/warranty plan, etc., so that if devices are destroyed, you can easily build a procurement list from which to order new equipment.

d. **License/Password Inventory** – Document all your software licenses and key passwords, and store them securely. In the middle of a restoration event, it is not a good time to realize that a device password has been lost, which is now preventing network access for the staff. Or even worse, finding that no one can find the license keys to the old payroll software that needs to be restored on a new server. Make sure to update the documentation when passwords are changed and new software is added.

e. **Key Vendor/Manufacturers Contact List** – Build a list of your key vendors (equipment manufacturers, software vendors, phone provider, Internet providers, IT consultants, etc.). Include names, phone numbers, 800 numbers, account numbers, and the like, in one place that is easily assessable if you need to reach out to them for assistance. Having that information readily available not only saves time, but keeps heads cool in a crisis, when you are needing your vendor's assistance the most.

6. Maintain Your System. One of the most important ways to avoid a disaster is by maintaining the security of your network. While fires, floods, theft and natural disasters may be unavoidable, and are certainly a threat, you are much more likely to experience downtime and data loss due to a virus, worm, or hacker attack. That's why it's critical to keep your network patched, secure, and up-to-date. Additionally, monitor hardware for deterioration and software for corruption. This is an often-overlooked threat that can wipe you out. Make sure you replace or repair aging software or hardware to avoid this problem. Many vendors force you to perform firmware updates before they will provide direct support of their systems – delaying your recovery.

a. **Patching and firmware updates -** Perform on a regular schedule and maintain a log for easy review of level and status.

b. **Asset lifecycle management** – Begin to create a process so that your systems can be supported/maintained in a reasonable manner by your vendors. Take end of life items out of your inventory and recycle them – do not leave in the rack or server room.

c. Warranties and Maintenance – Ensure you have warranties/maintenance on key devices and applications. Yes, it has a cost, it also protects you and aids in reducing resolution time when they are actually needed.

d. **Check your UPS systems at least once a year—Replace batteries every three years and replace the systems every five years with managed power options.** A properly sized and configured UPS solution can make a huge difference when those random power surges occur, or when hit by those short-term outages that plague many in Central Ohio. The right size and configuration can also help bring down systems in an orderly manner in the event of a longer-term outage, and allow for a faster recovery when the power is restored.

7. **Hire a trusted professional to help you.** Make sure you work with someone who has experience in both setting up business contingency plans (so you have a good framework from which you CAN restore your network), and experience in systems recovery.

8. **Validate your licensing/equipment configurations annually.** Review your licensing agreements with your application software annually. This review, along with updating your inventory, ensures that you maintain support on key applications, verify release versions (and maintain an agreed to "current level"), and allows you to understand software status and use location for better overall management.

9. **Ensure that your P&C insurance is updated annually to reflect your investment in IT systems.** Each year upon P&C business insurance renewal time, your insurance broker will ask your organization to complete an application for coverage. As a part of that renewal, there is an "IT" section that needs to be completed. Today, special attention should be paid to this area to ensure that you are compliant with requirements, understand your protection needs (cyber security coverage, customer access liability, lost revenue/business reimbursement, etc.), and to ensure your organization has the necessary coverage to be fully protected.

10. **Test, test, test!** A study conducted a few years ago by Forrester Research and the Disaster Recovery Journal found that 50 percent of companies test their disaster recovery plan just once a year, while 14 percent never conduct testing. If you are going to take the time and effort required to set up a plan, then at least hire an IT professional to run a test once a month to make sure your backups are working and your system is secure. After all, the worst time to test your parachute is AFTER you've jumped out of the plane.

How Affiliated Can Help

To help you protect your systems and be prepared for potential issues, Affiliated is offering you and your organization **a FREE Review Of Your Existing Disaster Recovery Plan.** This no-obligation review will identify areas that may be an issue now, those that could be problematic as you prepare your plans for the future, as well as show you how to align one of your key assets more closely to your business goals. We will meet with you to review your plan, and make recommendations on ways to ensure that your team can avoid pitfalls, and recovery quickly and effectively in the event of an emergency.

To request your review, call our office at (614) 495-9658 and ask for Jason. He will personally follow up to schedule your Free DR Review. Or you can send an e-mail to us at michaelmoran@aresgrp.com.

CRN MSP 500 2015

CRN MSP 500 2016

The Channel Company's CRN Managed Service Provider (MSP) 500 annual list distinguishes the top technology providers and consultants in North America whose leading approach to managed services enables their customers to improve operational efficiencies, realize greater value from their IT investments, and successfully leverage technology to achieve greater competitive advantage.