

# Ten Tips for Successful IT Disaster Recovery Planning

by [Paul Chisholm](#)

Businesses of all sizes rely on information technology as a crucial component of their day-to-day operations. Because data availability is a top priority, the need for companies to compile a thorough disaster recovery plan is essential.

According to Info-Tech Research Group, however, almost 60% of North American businesses do not have a disaster recovery plan in place to resume IT services in case of crisis - a recipe for possible business failure. Faulkner Information Services found that 50% of companies that lose their data due to disasters go out of business within 24 months, while the U.S. Bureau of Labor indicates that 93% are out of business within five years.

## Ten Tips for Disaster Recovery Planning

- **Devise a disaster recovery plan:** IT disaster recovery planning can be a daunting undertaking, with many scenarios to analyze and options to pursue. It is important to start with the basics and add to the plan over time. To begin, define what is important to keep the business running - i.e., email and application access, database back-up, computer equipment - and the "recovery time objective" or how quickly the company needs to be up and running post-disaster. Other key plan components to consider are determining who within the organization declares the disaster, how employees are informed that a disaster has occurred, and the method of communication with customers to reassure them that the company can still service their needs.
- **Monitor implementation:** Once a disaster recovery plan has been established, it is critical to monitor the plan to ensure its components are implemented effectively. A disaster recovery plan should be viewed as a living, breathing document that can and should be updated frequently, as needed. Additionally, proactive ongoing monitoring and remediation of processes, such as back-up data storage and data replication, results in fewer IT issues and less downtime should a crisis occur.
- **Test disaster recovery plan:** A 2007 eWeek survey of more than 500 senior IT professionals revealed that a whopping 89% of companies test their disaster recovery/failover systems only once per year or not at all, leaving their enterprises vulnerable to massive technology and business failures in the event of a disaster. An under-tested plan can often be more of a hindrance than having no plan at all. The ability of the disaster recovery plan to be effective in emergency situations can only be assessed if rigorous testing is carried out one or more times per year in realistic conditions by simulating circumstances that would be applicable in an actual emergency. The testing phase of the plan must contain important verification activities to enable the plan to stand up to most disruptive events.
- **Perform off-site data back-up and storage:** Any catastrophe that threatens to shutter a business is likely to make access to on-site data back-up impossible. The primary concerns for data back-up are security during and accessibility following a crisis. There is no benefit to creating a back-up file of valuable data if this information is not transferred via a secure method and stored in an offsite data storage center with foolproof protection. As part of establishing a back-up data solution, every company needs to determine its "recovery point objective" (RPO) - the time between the last available back-up and when a disruption could potentially occur. The RPO is based on tolerance for loss of data or reentering of data. Every company should back-up its data at least once daily, typically overnight, but should strongly consider more frequent back-up or "continuous data protection" if warranted.

- **Perform data restoration tests:** Using tape back-up for data storage has been integral to IT operations for many years, however this form of back-up has not been the most reliable. Today, disk to disk systems are gaining popularity. With either type of system, the back-up software and the hardware on which it resides needs to be checked daily to verify that back-up is completed successfully and that there are no pending problems with the hardware. With tape back-up, companies need to store the tapes in an off-site location that is secure and accessible, while disk systems need to have an off-site replication if the back-up is not run off-site initially. Moreover, companies need to perform monthly test restoration to validate that a restoration can be accomplished during a disaster.
- **Back-up laptops and desktops:** Although many companies have policies requiring employees to store all data on the company's network, it is not prudent to assume that the policy is being followed. Users often store important files on local systems for a host of reasons, including the desire to work on files while traveling and the need to protect sensitive data from the eyes of even the IT staff. Backing up laptops and desktops protects this critical data in the event of a lost, stolen or damaged workstation. Using an automatic desktop and laptop data protection and recovery solution is ideal.
- **Be redundant:** Establishing redundant servers for all critical data and providing an alternate way to access that data are essential components of an organization's disaster recovery planning. Having these redundant services in place at a secure, offsite location can bring disaster recovery time down to minutes rather than days.
- **Invest in theft recovery and data delete solutions for laptops:** IDC reports that more than 70% of the total workforce in the U.S. will be considered mobile workers by 2009. Accordingly, laptops are increasingly replacing the traditional desktop PCs. Unlike desktops, however, laptops are more easily misplaced or stolen, thus requiring organizations to secure data deletion and theft recovery options for their users' laptops. Theft recovery solutions can locate, recover and return lost or stolen computers, while data delete options can enable companies to delete data remotely from lost or stolen computers thereby preventing the release of sensitive information.
- **Install regular virus pattern updates:** IT infrastructure is one of those realities of business life that most companies take for granted. Companies often do not focus on email security until an incipient virus, spyware or malware wreaks havoc on employees' desktops. Organizations need to protect its data and systems by installing regular virus pattern updates as part of disaster recovery planning, which may even help prevent a crisis from happening.
- **Consider hiring a managed services provider:** For small- to medium-sized businesses, it is often cost prohibitive to implement a sound disaster recovery plan. Frequently these organizations lack the technical professionals to accomplish this. Managed services providers (MSPs) have emerged in recent years to perform this role. MSPs have the technical personnel to design, implement and manage complex disaster recovery projects. Additionally, MSPs have the server, storage and network infrastructure in place to manage a true disaster recovery plan. To keep costs manageable and make disaster recovery services, such as data storage and redundant servers, available to small- to medium-sized businesses, MSPs build shared, multi-tenant IT infrastructures that host multiple companies on the same hardware and network equipment which helps keep costs affordable and advantageous for its customers.

### **Future of Disaster Recovery Planning**

In determining the components of a disaster recovery plan, businesses typically need to make tough compromises, sacrificing the level of recovery (maximum amount of downtime and data loss) with cost. A relatively new form of technology - server virtualization - is beginning to gain popularity as a viable and cost effective means of achieving highly available, redundant systems. Server virtualization allows companies to consolidate multiple server functions on one host server, thus lowering total cost of operation and effectively managing emerging hardware advancements.

At first glance, server virtualization may appear to be risky and counter-productive when trying to achieve a highly available, redundant IT infrastructure. After all, server virtualization increases the risk of multiple server failures by housing numerous server services on a single host server. But, with the combination of hardware advancements and software ingenuity, companies will be able to capitalize on server virtualization as a practical and effective means to achieve disaster recovery.

In the case of a natural disaster or power outage that impacts a company's primary facility, a host server in a separate location connected to a SAN targeted for virtual server replication can be enabled quickly and with little effort. By capitalizing on increased virtual server performance as a result of software advancements and lower hardware costs with higher capacity, a robust and full-featured disaster recovery plan will be more readily attainable by more organizations.

### Bottom Line

Every business is vulnerable to experiencing a serious incident, preventing it from continuing normal business operations at any time. Beyond terrorist threats, less catastrophic events such as a lost or stolen laptop, the Northeast Blackout of 2003, Manhattan's steam pipe explosion in 2007, recent wildfires in California and numerous presently unforeseen possibilities can cause substantial business interruptions. Anticipating disaster and preparing seems both prudent and advisable, as does regular testing of IT services and back-ups.

A well-structured and coherent disaster recovery plan will enable companies to recover quickly and effectively from an unforeseen disaster or emergency, thus avoiding significant business interruption and loss.

---

### About the Author

[Paul Chisholm](mailto:paul.chisholm@mindshift.com) (paul.chisholm@mindshift.com) is Chairman and CEO of [mindSHIFT Technologies](#), a leading provider of managed IT services to small and medium-sized organizations. He was most recently President and CEO of COLT Telecom Group plc headquartered in London, England. Under Mr. Chisholm's leadership he grew COLT from inception to over \$1 billion in revenue and the company became the largest and most successful European alternative carrier.

## Network Disaster Recovery Plan in San Francisco Bay Area

Network Preventive	Disaster Measures	Recovery for	Plan IT	Team Disaster
-----------------------	----------------------	-----------------	------------	------------------

Preventive measures for business continuity usually involve a thorough **Disaster Recovery plan** that goes beyond a simple **network disaster recovery plan**. In light of current economic conditions, Activsupport understands that it's difficult to invest time and money into something that is only of use in the unlikely event that a disaster occurs. This may sound like a hard pill to swallow: however building a good Disaster Recovery plan may help an organization by more than just offering protection in the case of a flood or earthquake.

## Common situations that can be covered under a well-designed plan:

How many of us have had their ISP end their services over the past few months? Yes, a disaster recovery plan includes ISP contingency planning, and can be applied not only in the event of an earthquake, but also when a supplier goes out of business.

How fast and accurately can you document a claim that involves digital assets with your insurance carrier? A good disaster recovery plan can help you recover your losses more efficiently.

Disaster Recovery planning can be of use in many other ways, even as a competitive advantage. For example: As an insurance broker, imagine the following scenario: An earthquake hits San Francisco, communication is disrupted and businesses are struggling to turn their business continuity plans into reality in the disaster's aftermath. As an insurance broker your ability to communicate and process data at this time will be your greatest asset. Some businesses will contact their broker's only to find busy signals if any signal at all. However, if you have a well-designed Disaster Recovery plan you will come out well ahead of the competition. This could be a great way to differentiate your brokerage from another.

Basic Disaster Recovery planning includes procedures for backup & restore, user access, and security policies. As mention earlier, it can also include ISP contingency planning.

Network backup restore policies and procedures are probably the most basic elements of proper planning. However, many companies don't use any concrete methods for conducting daily, weekly, or even monthly backups. Many organizations don't even take the tapes offsite for safe storage. And what about those tapes? How do you choose a safe repository for your tapes? Which provider do you choose? How do you choose them? You may initially consider shipping the tapes out of the region in case there is an earthquake in the Bay Area. But what if it takes forever to get your data back from the provider when you really need it? How safe is your data in a repository anyway?

But backup is only part of the equation; organizations must also think about their internal policies with regard to where data is stored. Often many organizations don't monitor their employee's data storage habits. This leaves a great deal of important information on individual's desktops and on CD ROM's that may just be thrown in someone's desk drawer.

Disaster Recovery planning can be frustrating and difficult, seemingly an overwhelming task. If and when a disaster occurs, all the effort will seem worth it. The easiest way to develop a proper plan is to break it down to the most basic elements. Let's start with the easiest element, tracking down contributors. Having multiple directories is a must and having a few people responsible for making copies of the corporate directory every week to their palm pilot is a start. At least you will be able to contact your customers when your systems are down.

It's also important to think about the accessibility of your business systems. Can you access your business systems from the web? Are you using client server architecture? Will you be able to re-image your systems at a pre-selected location? Will you be able to get your data backup running?

When developing a plan it's important to remember that you're not just preparing yourself in the case of a natural disaster but also man-made ones too, such as security breaches. With the right plan you can avoid embarrassing and potentially destructive situations no matter which type of disaster you experience. This is why ActivSupport's Next Generation Disaster Recovery Planning services include a review of your current network disaster recovery plan and security efforts. We ensure that all efforts are made to protect your business no matter what happens. From earthquake to disgruntled employee, a proper network disaster recovery plan can prevent costly consequences.

Read on about Disaster Recovery Planning:  
[IT Disaster Legal Factors](#)  
IT Disaster Prevention

All of the insurance coverage mentioned in this article can be secured through Mr. Bob Marrone (Phone: 510-832-8000 x135), an excellent insurance agent that we have worked with for over 6 years and helped us write this article.