Ten Key Steps to Surviving & Succeeding After an IT Disaster

Taking action with disaster preparedness and disaster recovery

by Tom Fischer, CEO and founder

TECA DATA SAFE

Summary

For any organization dependent upon its IT for day-to-day operations, planning for disaster has become a critical component for ensured ongoing success. In fact, for any organization it should no longer be a question of *if*, but rather a matter of *when* an IT disaster will strike and threaten continued operations or even the organization's very existence.

As many have discovered, disaster encompasses more than floods, fires and tornadoes. Threats to IT infrastructure — including power outages, technical glitches, malware and viruses, and even the malfunctioning of just one server — all have the potential to prove catastrophic. When an organization accepts this reality and plans for it accordingly, downtime is minimized and recovery is much more certain and successful. Planning and preparing are vital to the recovery process, while employing best-of-breed technology is essential as well.

When it comes to IT disaster recovery (DR), studies indicate those organizations that enjoy "best-in-class performance levels" share several common characteristics, including a realistic perspective on the cost of downtime versus the cost of IT backup/disaster recovery tools and processes; senior management involvement; a formally documented IT disaster recovery plan; testing; training and annual (or more frequent) review.[1]

When an organization accepts this reality and plans for it accordingly, downtime is minimized and recovery is much more certain and successful.

Challenges

Unprepared for Disaster

Most organizations have some form of IT disaster preparedness in place. Too often though, they are reliant upon outdated systems or untested backup plans. Even in this age of advanced technology, the full extent of recovery preparation for many organizations remains backing up data to tape, and then taking that backup offsite. Unfortunately, many of these organizations have never tested their backups by attempting a system restore. What's more, access to a tape taken off site is not only questionable, it also poses a security risk. When disaster inevitably strikes, these organizations discover their backup strategy was lacking, and that they are facing lengthy downtimes, as well as staggering costs to restore their systems, applications and files.

Disasters come in multiple shapes and forms. From natural disasters that impact an electrical power supply, to fires, system failures or software glitches. Even if the impact is limited to internal systems, intranet, email and order processing interruptions can significantly damage and even cripple a business.

Solutions

Before Disaster Strikes

Whether it is a flooded building or a fire in the computer room, the *type* of disaster that brings a business to a halt is irrelevant to IT restoration. Rather, it is the preparedness of the organization to face threats *before* they happen that will determine the success of disaster recovery. "Defining and deploying a successful IT disaster recovery plan to minimize business interruptions requires a combination of strategic actions, organizational capabilities and enabling technologies." [2]

Any organization serious about formulating a successful IT disaster recovery plan should perform the following ten key steps to ensure effective restoration after a disaster, and the certainty of ongoing business capabilities.

1 Calculate the cost of downtime

When it comes to seeking a solution, an organization must first fully grasp the magnitude of the problem. As such, it is essential to perform a realistic calculation of the cost of downtime. Utilizing a downtime calculator to make this determination will offer a clear perspective on the sizeable costs associated with a business that can no longer operate as usual. In this way, an organization's C-level can fully appreciate and realize the value of a strategic IT disaster recovery solution, as well as accurately determine the investment that should be made for its implementation.

2 Plan for recovery time objective

How long can an operation tolerate downtime before it becomes catastrophic to business? Planning a Recovery Time Objective (RTO) begins with determining a timeframe. For example, if systems are down for a week, is that acceptable? Or, can the organization only afford one hour of downtime before it becomes critical for operations to resume? To determine this number, interviews of people within the organization should take place in which individuals assess business functionality, productivity and ability to continue to service customers when IT is down. It is crucial to define realistic goals and to have reasonable expectations about recovery time. Once an organization has determined RTO, they should seek a solution that fits their needs.

3 Establish recovery point objectives

Recovery Point Objectives (RPO) establish a recovery point. This is determined by establishing the time of the last backup or imaging of apps and data before the disaster occurred. Anything that transpired between the time of that backup and the actual disaster may be lost. The question then must be, is that acceptable to the organization? Can any of the data that has been lost be recaptured or re-entered manually? If those are not acceptable solutions, the organization will need to explore other options.

4 Appoint an executive sponsor

While IT disaster recovery planning calls for the input and participation of the group, it also requires that someone take on a leadership role. Appointing an executive sponsor (ES) puts a decision maker at the forefront of DR planning. The ES is someone in a position of authority who appreciates the serious need for DR, and who can also allocate time and money resources to spend on the issue. Maintaining executive oversight keeps the C-level involved and in touch with the process.

5 Perform a realistic assessment

Organizations should review current DR plans and assess where there might be gaps in strategy. Have they tested the current plan? Do they know how long it will take to recover/restore systems? Have they determined which systems are critical to ongoing business operations? Would it be catastrophic if they were lost? Developing this plan effectively may require the assistance of a DR professional.

6 Develop a plan of action

Organizations should examine multiple factors when developing a plan of action. For example, what are the various recovery scenarios? Is there a way to establish a messaging system to alert the ES and IT team to a system failure? Does the DR plan involve backup resources and infrastructure on which to run apps and data? Does it require components to backup offsite and to the cloud? A DR plan of action can be time-consuming and difficult to assemble, but is absolutely critical to successful restoration of systems following a disaster.

7 Test, test and test again

Trial runs and drills are necessary, as an organization must know the DR strategy is effective. When testing the system, issues and gaps will reveal themselves, thus allowing the organization to pinpoint shortages of resources in infrastructure or planning, and make adjustments accordingly.

8 Track results against your plan

Once the DR plan has been implemented and tested, an organization can ascertain if there are any issues and how they plan to address them. For example, were all critical files, data and applications backed up? If not, what went wrong? How will this be addressed? By tracking results against the plan, an organization can continually make improvements.

9 Train staff

Once the plan is established and put into place, the entire staff needs to understand the crucial part they each play in an organization's IT disaster recovery. A program of initial staff training, along with continuing education should be implemented as a component of the overall process.

10 Set an annual review

No business is static. That's why DR planning needs to change and adapt as well. Over the course of a year, systems may have been added or removed; capacities may have increased; personnel changes may have occurred. A DR plan needs to compensate for all these factors. Therefore, once each year, an organization should review the DR plan and strategy, and make changes wherever necessary.

… it should no longer be a question of *if*, but rather a matter of *when* an IT disaster will strike and threaten continued operations or even the organization's very existence.

A Trustworthy Disaster Recovery Solution

TECA Data Safe, innovators in IT backup and disaster recovery, offer small- to medium-sized businesses the ability to meet the challenges of developing and executing a comprehensive IT disaster recovery plan by offering proven services, components and industry-renowned expertise.

By providing a downtime calculator online, TECA gives organizations the ability to calculate the cost of downtime as a result of an IT disaster. The total monetary costs associated with unexpected downtime can be very sobering, and as such, TECA advises businesses to use this information as part of a risk analysis when considering the cost of an IT disaster recovery solution. More often than not, the results indicate the necessity of taking preventive action.

Even when a backup system is in place, data recovery can prove to be problematic for many organizations because of data that may have been entered into a system after the last backup and prior to the disaster. The result is often serious and potentially permanent critical data loss. Fortunately, TECA has the ability to meet an organization's recovery point objective, whether it is to the previous backup or even to minutes prior to the disaster.

Additionally, when an organization is developing their overall DR strategy, it is wise to consider offsite backup and recovery options. TECA offers organizations a completely integrated IT disaster recovery solution known as Rapid Rebound. Rapid Rebound enables a return to business after a disaster in as little as 6 to 24 hours. With TECA's Rapid Rebound service, a virtualized backup appliance is placed at the organization's site which then replicates backed up applications and data to the cloud, TECA's secure data center offsite.

Finally, organizations should prioritize annual testing as an integral part of their DR strategy. Testing should pinpoint issues with connectivity, spotlight gaps in technology strategies and expose any missed data. TECA's testing provides organizations with a thorough perspective of their DR strategy along with documentation that will guide an organization in developing corrective measures. As a result, organizations maintain confidence in their ability to recover from any disaster.

Conclusion

As IT systems have become a ubiquitous part of business today, dependence on consistently functioning IT systems mandates that organizations develop effective IT disaster preparedness and IT disaster recovery strategies. However, when the business is small to medium in size, often the IT department is limited in scope, and sometimes may not even exist at all. Given these circumstances, the need for a DR strategy is even more urgent. Ultimately, DR planning and preparation will ensure minimal downtime and a timely recovery back to business.

Following the ten steps to surviving and succeeding after an IT disaster offers organizations the tools to maintain continuity, along with peace of mind in the knowledge that natural or manmade disasters do not have to mean a business catastrophe.

TECA Data Safe Corporation
11670 Fountains Drive
Suite 200
Maple Grove, MN 55369

1-888-398-6235

www.tecadatasafe.com

[1] Csaplar, Dick. *Disaster Avoidance and Disaster Recovery: Making Your Datacenter Disaster Resilient;* Aberdeen; May, 2010.

[2] Ibid.

TECA DATA SAFE