Chapter 9—Cracking Disaster Recovery

During disasters, the main super villain of IT attacks is Outage. He is the business destroyer. In February of 2010, two back-to-back blizzards slammed the entire northeastern United States. The storms dropped more than four feet of snow in some areas and caused the shutdown of all government agencies in the capital. In New York, the Long Island Rail Road reported that commuter traffic was down by more than 46 percent. As many as a million people were prevented from going to work due to the weather. Businesses, government agencies, schools, and universities were all shuttered. Several estimates calculated that in the government sector alone more than $100 billion in productivity was lost. There is not a clear calculation of lost productivity in the private sector, but it conceivably topped the $250 billion mark.

Major events such as the terrorist attacks of September 11, 2001; the 2003 blackout in the northeastern United States; Hurricane Katrina; and the California wildfires are other case studies in the need for developing comprehensive disaster recovery plans. These are unusual events. They make headlines because they are dramatic and all-encompassing and they are also the exception. Disasters of such widespread and long duration are few and far between. But, in all these events, many businesses were stopped in their tracks with no recourse to continue doing business for weeks at a time. Some ended up closing their doors because they could not recover. They needed disaster recovery plans *before* an event occurred. Many companies lost access to their facilities completely for days or even weeks at a time, and for a few unlucky companies their location was badly damaged or even destroyed.

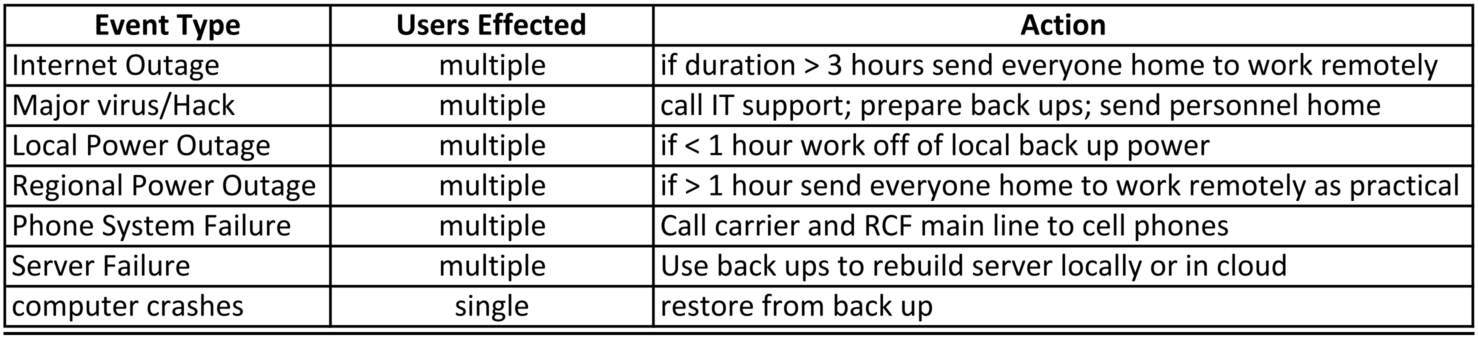
Every business needs at least basic disaster recovery protection, but many small businesses do not have the resources to develop a major disaster recovery plan that can take into account all scenarios. When resources are limited, a more pragmatic approach is necessary.

The number one goal of a disaster recovery plan is to preserve the profitability of the business when something goes wrong. The actions taken will generally depend on the type of disruption and the duration. A few basic precautions can go a long way toward maintaining the viability of the business.

Think of DR as active insurance. You are taking pragmatic action—not just a financial hedge toward alleviating the damage an event can cause you and your business. With that in mind, there are three areas businesses need to focus on in their disaster recovery planning: voice, data, and computing. Voice is generally the first line of communication with customers. It encompasses the company's phone numbers and phone system. Data is the company's vital information: digital documents, customer information, financial information, etc. It is the life blood of the company and by far the most difficult to replace if lost. Last, but not least, is the company's computing power. It is comprised of the laptop and desktop computers of the company, as well as the network equipment that enables them to run and connect to the Internet and one another.

More than one type of DR plan is necessary. Each plan is scenario and time based and addresses the company's reaction to a specific disruption in one of the three areas. It will also encompass individual and company-wide needs. The depth of planning and the resources required are dictated by the needs of the company and the cost of an outage. For example, a financial company engaged in high frequency trading may invest in fully redundant systems to prevent even one minute of disruption. In some cases they may even purchase alternate office space that is ready to be occupied on a moment's notice. While in contrast, a professional services company whose primary function is person to person may make very little investment and take relatively simple steps to alleviate an outage.

A DR planning matrix is an easy way to get started. The most common disruptions that need planning are file server issues and Internet outages.



Event Type	Users Effected	Action
Internet Outage	multiple	if duration > 3 hours send everyone home to work remotely
Major virus/Hack	multiple	call IT support; prepare back ups; send personnel home
Local Power Outage	multiple	if < 1 hour work off of local back up power
Regional Power Outage	multiple	if > 1 hour send everyone home to work remotely as practical
Phone System Failure	multiple	Call carrier and RCF main line to cell phones
Server Failure	multiple	Use back ups to rebuild server locally or in cloud
computer crashes	single	restore from back up

Data Planning: Where data is located and how it is accessed matters. For instance, companies that move 100 percent to a cloud model accept loss of access risk during Internet outages. Internet availability becomes a single point of failure. Some companies will invest in purchasing a redundant connection from a different provider to alleviate the risk of Internet loss. Others choose a hybrid cloud-premise model where a cloud server is linked to a local file server. If the local server has issues the backup server can be accessed through the connections. Many times cloud servers can provide a poor user experience due to latency and bandwidth issues.

A redundant server is different than data back up! Data backup is normally accomplished with versioning over time to provide the ability to restore a file from a previous point in time weeks or even months before the current version. Tape backup is dying a slow death and being replaced by low cost local and cloud storage.

Computing Planning: The ugly truth is that over a long enough timeline, all equipment fails. And even worse, predicting the time of failure is nearly impossible. Anything can happen—drops, spills, theft, or just bad luck and the drive fails. Whatever the cause, you must plan for your next replacement computer now. As a rule of thumb, computers will need to be replaced every three to four years.

Telephony Planning: Widespread use of cell phones has made planning for telephone issues much easier. The simplest plans just direct customers and staff to alternate phone numbers. Depending on the business, in the case of call centers, user groups, etc., very intricate telephony planning is possible with remote call forwards to redundant locations and back up lines if required.

How to prepare?

- Keep a record of your software licenses and types of software on the computer.
- Keep a record of where your software copies are stored (physically or digitally).
- Record the serial number of your computer and warranty information.
- Ensure data is backed up on the company server or directly using a backup client.
- Keep records of all passwords: computers, firewalls, servers, switches, domain controller, etc.

It is helpful to keep at least one physical copy of all information. If you have a general event and all the records were digital you could be in trouble.

Disaster recovery planning is mostly common sense. The most important thing is to think through scenarios by duration. By planning for the worst in advance, the chances of staying in business after a disaster are greatly improved. The next step is to evaluate what company to assist you in your expertise gaps. It begins with choosing the right partner and understanding *Outsourcing Secrets.*

Clues to Cracking the Code

- Start with the company backups. Data is the most difficult asset to replace or recover.
- Do not be intimidated by technical jargon. Keep it simple. Continuously ask yourself the question, if X happens, how does it affect our business?

Planning for hardware refreshes on a schedule will greatly reduce the need, and therefore cost, of initiating a major disaster recovery operation.