SEVEN Components of a Successful Disaster

Why seven you ask? I would like to tell you there was deep thought put into the title but really, it was simply a matter of outlining the framework on how to be successful should your credit union ever experience a disaster and it comes down to seven key components.

In 1949 Edward A. Murphy Jr., a rocket engineer for the United States Air Force was involved in testing human acceleration tolerance at Edwards Air Force Base. Mr. Murphy was tasked with creating the 16 accelerometers which were to be attached to the human subject in this experiment. There were two different ways each sensor could be glued to its mount. During the test, it was determined that every single accelerometer was put on the wrong way. Mr. Murphy blamed it on his technician, stating, “If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it.” The more popular term we are familiar with is Murphy’s Law: “If anything can go wrong, it will”.

There are so many possibilities, so many things that can go wrong. The key is to put your credit union in the best possible position for success. That is the purpose of SEVEN Components of a Successful Disaster.

Component One: Impact Analysis

Step one of a successful disaster is to define “success”. What does success look like for your Credit Union? Simply surviving a disaster does not constitute “success”. The effects of a disaster can reach far beyond the recovery.

A few years ago we had a customer in Louisiana declare a disaster after hurricane Isaac passed through their state. Having already been through Hurricane Gustav in 2008, they understood the impact a regional disaster could have on a community. We worked with the credit union to put measures in place to back up their core and ancillary systems to our data center in Oregon. We had vendor connectivity in place for their ATM’s, shared branching and Internet Banking, along with branch communications. The credit union also tested on an annual basis.

When Hurricane Isaac hit, they were prepared. Not only were they prepared, they were the first financial institution up and operating in the community. Their members were extremely grateful they had access to their funds but more so, the entire community was appreciative. The vice president shared with me how touching it was to have various people in the community come up

to them while withdrawing money from the credit unions ATM's and thank them for being accessible in a time of crisis.

Because of the credit union's availability to the community, not only did they increase member loyalty, they experienced a considerable increase in membership.

I am sure you've heard the idiom, "one's loss is another's gain"? There are statistics splashed all over the internet citing 80% of businesses that experience a major disaster go out of business within 18 months. I can't speak on this statistic since I've never come across a credible source. However, I can speak directly to the fact that if this credit union gained members, someone else lost them.

Defining success requires involvement by credit union leaders, including IT determining the implications of a short, medium and long-term disaster. It is important to remember that not all disasters are the same. They can range from a single server, controllers failing in a SAN that brings down the entire virtual environment, communications failure, to total destruction of the data center and anything and everything in between. Over the years, I have seen every one of these scenarios occur at one time or another.

By the way, earlier I mentioned Murphy's Law. Not only did it originate at Edwards Air Force Base but Edwards Federal Credit Union happens to be a customer of ours. In 2013, they lost their processor board and were forced to declare a disaster. However, I am happy to say, they were well prepared and they experienced a successful disaster **(see case study on website)**.

Component Two: Needs Assessment

Now that you've defined success, you need to determine specifically what components need to be up and operational in order to achieve success. This requires building a team that includes representatives of all major departments in your credit union.

I've gone onsite to credit unions to review and discuss their current disaster recovery setup and you should see the eyes of management in various departments when they find out some of the key functions of their day to day operations would not be operational in a disaster. I cannot emphasize this enough: It cannot be left up to IT to determine the critical needs of each individual department.

Many credit unions focus on their core system, but networks have become highly complex. There are many different components necessary for a successful recovery. I can't tell you how many times we've requested a list of the components a potential customer wants protected and they include their core, Exchange, etc., and completely omit the domain controller; or, they list all of their key servers and omit third-party vendor connectivity. It is imperative to understand the interdependencies of the various components.

In this day and age, more members are accessing their funds via ATM and Debit Card and managing their accounts via internet banking or mobile than brick and mortar. Also, bills and payroll are primarily coming in via ACH. During a major regional disaster, most members will be evacuating the area and ATM's and Debit Cards will be their only form of transacting. Waiting until a disaster occurs is not the time to realize you overlooked some key components.

It is important to understand that assessing your needs is not a one-time event, it should be done on a regular basis. We don't turn 40, go to the doctor for a checkup and, assuming everything checks out fine, never return. You have to be diligent. You have to regularly assess your needs. I have never come across a credit union where their technology and staff were static. Equipment will become outdated and need to be replaced, new technology will be implemented, vendors will be replaced and staff will turnover. It's just a fact! Your credit union will be forever changing and evolving, so, therefore, re-assessing is a must. If that sounds daunting, it can be, at least initially. However, it becomes much easier to reassess once you have assessed.

Component Three: RTO's & RPO's

What are RTO's and RPO's you ask? RTO stands for Recovery Time Objective, which defines the acceptable amount of time you are willing to be down. Since there are so many moving parts in a recovery, this is very granular. Each and every component will need to have a defined RTO.

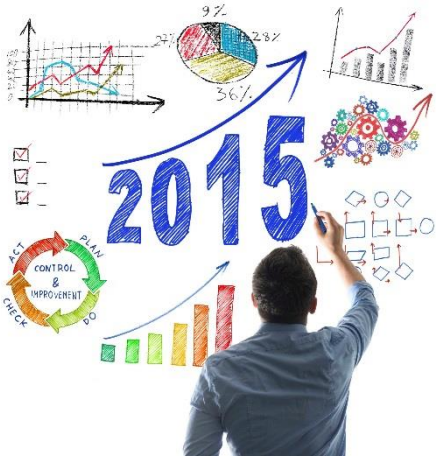
RPO stands for Recovery Point Objective. In a nutshell, this is the amount of data you are willing to lose, if any. For example, if a server crashes in the middle of a business day, are you ok with recovering to last night's backup and losing everything that has occurred since, or do you need to recover to the point at which you went down?

RTO's & RPO's are as important as any other component for a successful recovery. In fact, it is a key tool in measuring success. Let's say you perform an annual disaster recovery test. At the end of day two, you are finally able to get your core system up and operational and although the system is recovered, it is from the prior night. To break this down, it took 48 hours to recover your core system and you have lost all of the transactions that occurred leading up to the simulated disaster. Furthermore, if this was an actual disaster, you would have had to play catch-up for the two days you lost. Does this constitute a successful recovery? Can you sleep

comfortably at night with these results? No, of course not. By defining RPO's and RTO's you can effectively measure success while testing. If you are unable to meet the objectives, you can then reassess and incorporate changes where needed. An example would be replacing recovery via backup with real-time replication to improve RPO's and RTO's.

Whether you choose to staff up, invest in additional hardware, software, communications etc., and be responsible for your own recovery, or outsource to a service provider, defining the RTO's & RPO's is going to help you determine the actual cost. The more aggressive you get with RTO's & RPO's the more you can expect to pay. However, it's critical to define your objectives before you can truly determine if this is something you can afford to do on your own or if outsourcing makes sense.

Component Four: Cost Analysis



You now know what our vision of a successful disaster looks like. You've assessed our needs and you have defined the RTO's and RPO's necessary to meet the overall objective. You now need to outline how much you should spend in order to achieve the desired results.

Many credit unions allocate significant portions of their budget to sell and market the services that generate the most revenue. Unfortunately, for many, IT is not considered a revenue generator. Many credit unions, especially those which have never experienced a natural disaster, security threat, or human error, struggle to justify spending on disaster recovery.

Disaster recovery spending is insurance against the risks of user downtime, data loss, and business interruption. While life insurance, health insurance, and homeowners insurance are pretty much a given, it's difficult to assess how much coverage is enough, and how much to spend.

IT managers face the same issues in planning and justifying disaster recovery spending. While every credit union knows it needs some level of protection, determining the extent and the appropriate financial investment is an ongoing challenge.

Credit Unions don't just hand money to anyone. They have a formula for determining the level of risk. They factor in the credit score, time-on-job, annual income, etc. Depending on the type of loan, they may even require the member to purchase insurance. All of this is done to mitigate the risk on the investment. Determining the appropriate financial investment for disaster recovery should be treated no different.

Disaster recovery is competing with new business applications, security solutions, migrations and upgrades, operations and maintenance, and IT cost reduction projects for a share of diminishing IT budgets. The challenge for IT managers is assuring that spending remains at adequate levels so they're ready, should the unlikely occur, and that important new technology, training and processes are implemented to mitigate or recover quickly from realized internal and external threats.

Unplanned Downtime (Mission Critical)	Typical Uptime	Hours Down per Year	Cost per Unplanned Downtime Hour	Downtime Risk
Average	98%	175.00	$42,000	$7,350,000
Very Good	99%	87.60	$42,000	$3,679,200
Outstanding	99.5%	43.80	$42,000	$1,839,600
Best in Class	99.9%	8.76	$42,000	$367,920

Figure 1: Typical downtime risks for various availability levels. Note that a 1% increase in availability translates to more than $3 million in value. Comparing the cost of the disaster recovery plan with the risk mitigation value allows IT managers to make valuable spending decisions, and justify additional investments in disaster recovery solutions.

To determine how much disaster recovery spending is needed, IT managers should perform a three-step analysis:

1. Assess the downtime costs for crucial business systems
2. Calculate the potential disaster risks and impacts
3. Compare alternative plans to determine benefits of each proposed solution, and how much spending is enough.

This review helps put the risks, possible projects, and benefits into perspective. Being systematic helps executives make the right spending decisions, and justify the disaster recovery investments against other competing IT projects.

Component Five: In-House vs Outsource

Ok, let's recap. You've defined what a successful disaster looks like, the components needed for recovery, how much time you are willing to be down and how much data you are willing to lose, and you've established a budget to accomplish all of the above. Now, you need to determine who exactly is going to perform all of these duties. Basically, you have two options or a variation of the two. You are going to either go in-house by hiring additional staff, purchasing the necessary infrastructure, etc., or you are going to outsource, by hiring a service provider to provide the infrastructure, technical resources, etc. Of course, there is always the third option of a hybrid approach, where you in-house a portion and outsource the remainder.

In-House

Do you fully understand the business impact of downtime by application?

In order to confidently say “Yes” to this question, you need to have:

• Performed a business impact analysis (BIA) to help you prioritize applications based on their importance to your credit union.
• Used the BIA to help you prioritize applications.
• Mapped application inter-dependencies (so that you have a clear picture of which applications depend upon each other and tier them correctly.)
• Set applications’ Recovery Time Objectives and Recovery Point Objectives (RTOs/RPOs) accordingly.

Can you afford to do IT disaster recovery in-house?

Answering “Yes” to this question means you have both the necessary capex and opex budget to support an in-house IT disaster recovery program. On the capex side, you’ll need to fund DR equipment and software, as well as recovery sites and systems for the recovery site. (Can you say, “I need two of everything?”)

On the opex side, you’ll need to pay for recovery site operations, staff time to develop recovery procedures and maintain recovery manuals. You’ll also need to fund the once or twice a year travel and other expenses for proper DR testing. It definitely adds up.

Do you have the in-house expertise for DR?

Keeping systems up and running is an entirely different skill set than recovering them quickly from scratch during a disaster or after a disruption, and many CIOs do recognize this. Sungard recently did a survey of Fortune 1000 enterprises on their DR planning efforts and concerns, and 54% mentioned shortages in staffing and expertise as their biggest challenge. Having worked with many credit unions, they struggle with this on a day to day basis. The key questions CIOs need to ask themselves are:

• Does my staff have the skills to develop recovery processes and procedures?
• Can they perform rigorous change control?
• Are they actively up-to-date on DR best practices and integrating them into the IT lifecycle?
• Can they perform robust DR planning and manage a fail-proof disaster recovery program?

Are you confident you are recoverable?

The key question here for CIOs to answer is: Am I able to stand in front of the Board of Directors and certify that the credit union is recoverable? Below is a directional checklist for being able to say a resounding “Yes!”

• We actively test and validate our DR plans.

• We have a good handle on change management (and perform it regularly).

• Our staff is willing and able to travel in the event of a disaster.

• We can prove recoverability in an audit.

• In our last test, we met all RTOs and RPOs for our mission-critical applications

So should you outsource your IT disaster recovery program to an outside provider? That depends on your overall IT strategy, your desired availability posture, and of course, your answers to the foregoing four questions.

Outsource

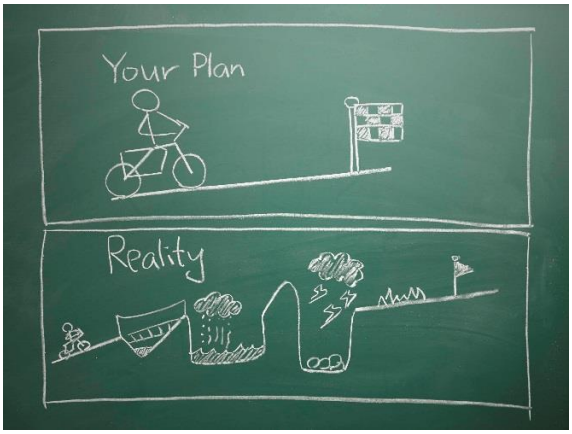
It is critical that you properly vet your potential disaster recovery vendors.

- Do they fit into your budget?
- Are their services inclusive of all of your needs or only some?
- Can they meet your RTO's and RPO's?
- Do they have industry and core system knowledge?
- Do they provide a no cost/ no obligation evaluation of their services?

Outsourcing disaster recovery can make a lot of sense. However, it is one of the single most important decisions you are going to make. So, it is critical the vendor not only fits into your budget but is capable of delivering on their promise. Make sure you are able to evaluate their products and services.

If the vendor is not willing to take the time and show you they are capable of delivering on their promise prior to signing an agreement, then you might consider looking elsewhere. The last thing you want to do is put in the time and money implementing the service, only to find out later during a test or an actual disaster, they cannot deliver. You might not get a second chance.

Component Six: Reassess



Now you've determined what a successful disaster looks like. You also know specifically the components needed for recovery. You have also established RTO's and RPO's. Additionally, you've established a budget and determined whether to go in-house or outsource. You should be proud of your efforts, you've accomplished a lot and are getting very close to meeting your goal to achieve a successful disaster, should one occur.

You are now at the point of reassessing. Reassessing is necessary because although you've determined what a successful disaster looks like, the components necessary for recovery and your RTO's and RPO's, it may not be realistically possible within your budget. You may now need to adjust your budget or your plan.

- Did your needs assessment include only the most critical servers or did you add servers that are non-critical, just desirable?
- Are your RTO's and RPO's too rigid? Can you loosen things up a bit?
- Does your core really need to be up in 15 minutes or can you live with a 4 hour RTO?

- Can you afford the capex and opex necessary to do it on your own or does it make financial sense to outsource with an opex model?

There are many questions that need to be asked as you reassess. If you choose to outsource, it's important to properly vet each vendor and ensure they can deliver on their promise, which includes a thorough evaluation. Additionally, does your vendor offer recovery tiers based on RTO's and RPO's? If you have servers that are important but do not necessarily need to be up and running within the first 24 hour window, does your vendor offer price breaks for extending the RTO's and RPO's?

Once you've sifted through all of the information you have gathered, you are in a much better position to determine the best direction for your credit union. The idea is to do your due diligence so you can feel confident in the decisions you make.

Component Seven: Test, and Test Often

Once you've implemented your disaster recovery solution you are on the right track towards positioning your credit union for success in the event of a disaster. However, IT is not static, it is ever changing. Therefore, it is important you implement the processes to adapt as circumstances change. Whether it's an upgrade to existing servers, additional servers, changes to third-party vendors, or adding or removing branches, you need to have procedures in place that streamline the DR process.

On many occasions, during tests and even in actual disasters, we've encountered customers who have made changes and neglected to notify us. This oversight can be the difference in experiencing a successful disaster, and as I have already mentioned, you may only get one shot. By putting the proper procedures in place, you can avoid this by ensuring when you upgrade or add equipment and services, disaster recovery is always included on your check-off list.

It has become so commonplace that we implemented a process ourselves to send out a notification to our customers throughout the year, reminding them to review their DR services to ensure there have not been any changes that would affect their recovery. Additionally, we do a pre-DR test meeting to discuss and review both expectations for the upcoming test and their existing services to ensure nothing has been overlooked. Nobody wants to wing-it during a disaster. Preparation is key.

Now that you have clearly defined RTO's and RPO's you have a quantifiable way of measuring success during a test. Whether you are going with an in-house solution or outsourcing, you must ensure you keep track of your recovery times. This isn't to say that by not meeting your RTO's your test has failed. It simply allows you to determine if expectations are set too high and need adjusted, or if a different recovery method is required to meet the RTO.

As you proceed through a test, it's critical you thoroughly document each individual process being recovered. Having detailed documentation allows for a post-DR test review to evaluate and determine if the recovery procedures were effective or if adjustments are needed.

Since a disaster is unpredictable, it's important that you vary your disaster test scenarios. Many times, credit unions have a standard script they run through when performing their test. To be most effective, and increase your chances of success, you must enter each test simulating scenarios that are most likely to occur. For example, if you are located in the south east, you may want to simulate the effects of a hurricane or tornado. If you are in the Midwest, maybe a tornado or flood. And if in the west, maybe an earthquake or flood. However, don't overlook a Murphy moment, a random scenario such as the failure of a single server or an irate employee wreaking havoc in the computer room.

Also, in large regional disasters, you may not have access to your entire IT staff. Even during hurricane Katrina many police and firemen did not show up to work because they were taking care of their family. This is a likely scenario, so you need to be prepared to function with minimal staff. If outsourcing, selecting a vendor that understands your business is a very real consideration and if you choose to go in-house, having adequate staff, cross-trained and working outside of the region will be required.

As you look at the various types of disasters it is clear to see there is a significant difference between a disaster where the data center is completely out of commission versus a single server recovery where routing of inter-dependent servers and third-party communications is needed.

With so many natural disasters making the news, disaster recovery has moved to the forefront for many auditors. However, this really isn't as much about passing an audit as it is keeping your credit union in business and ensuring your members are able to access the funds they entrusted your credit union to protect. Without thorough testing on a re-occurring basis, you are playing a guessing game on whether or not you will be able to successfully recover from a bad situation.

So, there you have it! Disaster recovery is very complex. However, with the proper components in place, should the unforeseen occur, your credit union will be well prepared to experience a successful disaster.

Information Management Solutions
808A NW Buchanan Ave.
Corvallis, OR 97330
www.cusolution.com
(888) 356-6043