

FRSecure White Paper

10 Disaster Recovery Best Practices

Prepared By:
Evan Francen, CISSP CISM
Managing Partner
FRSecure LLC
evan@frsecure.com

10 Disaster Recovery Best Practices

Table of Contents

Table of Contents	2
Introduction	3
Best Practice #1: Account for all Stages of the Cycle	3
Normal Operations	3
Disaster Event	3
Disrupted Operations	4
Disaster Restoration	4
Restored Operations	4
Reconstitution Process	4
Normal Operations	4
Best Practice #2: Engage the Business	4
Senior Management Sign-off and Funding	5
Planning Group	5
Business Impact Analysis	5
Best Practice #3: Define the Scope and Objectives	6
Conduct Comprehensive Inventory	6
Establish Priorities	6
Best Practice #4: Understand Systems and Dependencies	6
Best Practice #5: Offsite Data Storage	6
Best Practice #6: Don't Forget Support Data	7
Best Practice #7: Update Continuously	7
Best Practice #8: Use Checklists	7
Best Practice #9: Test, Test, and Test	7
Best Practice #10: Store Plans Offsite	8
Bonus Best Practice: Don't Forget about Security	8
About FRSecure	8

10 Disaster Recovery Best Practices

Introduction

Every company has a disaster recovery plan, right? I wish this were so, but the reality is that many companies do not have disaster recovery plans. Even many of the companies that do have disaster recovery plans fail to update and/or test them regularly. This white paper is intended to help people responsible for disaster recovery planning understand some of (not all of) the best practices when it comes to disaster recovery planning. Some of the information in this white paper is basic, but so are many of the critical practices involved in disaster recovery planning. Why complicate things if the basics are missing?

The information you will find in this white paper is largely based upon firsthand experience gained from working with many of our client companies. We do not disclose our client names as a matter of policy. This white paper is written to communicate ten best practices and is not intended to be a step-by-step guide.

Best Practice #1: Account for all Stages of the Cycle

There are six stages in a disaster recovery cycle and a disaster recovery plan must account for all six stages. Most companies account for three or four of the stages, but not all.

Normal Operations

This is obviously where a company wants to be at all times, in a perfect world. All systems are running smoothly and few, if any outages are reported. The disaster recovery plan should capture this moment in time in as much detail as is feasible.

Disaster Event

This is usually an abrupt event that leads to a serious and sustained disruption to normal business operations. The definition of a “disaster” and who can declare a “disaster” must be contained in a disaster recovery plan. Your disaster recovery plan should take as many foreseeable disaster events into account as is feasible. For instance, if your company has only one site located in the Midwestern United States, the following natural disaster events should be accounted for, at a minimum:

- Tornadoes
- Flooding
- Fire
- Severe Thunderstorm
- Hail
- Snow/Ice/Blizzard
- Viral Outbreak

In addition to natural disasters, human-caused disasters should be accounted for such as:

- Sabotage
- Terrorist Act
- Infrastructure Failure (Power)
- Infrastructure Failure (Telecommunications)
- Infrastructure Failure (Bridge and Road)
- Riot

10 Disaster Recovery Best Practices

- Labor Stoppage

The potentially disastrous events listed above are not all inclusive. Use statistical data whenever possible to decide which disaster events apply to your company and the risks they pose.

Disrupted Operations

If a disaster event occurs, but does not disrupt operations, then it is not a disaster in terms of disaster recovery planning. Only if there is a disruption of operations is a disaster declared. The extent and impact of the disruption is what dictates a response. A disaster recovery plan should define what “disrupted operations” means and who decides when a response is warranted.

Disaster Restoration

At this point an event has occurred that has disrupted operations significantly enough to have declared a disaster. The disaster recovery plan is activated and restoration procedures are enacted. It doesn't matter if restoration takes place in a remote location or if restoration takes place locally, the restoration procedures should be as detailed as possible for both scenarios. Answers and procedures that address the what, where, when, how, and by whom of the restoration process must be included in the plan.

Restored Operations

At what point are business operations determined to be operational *enough* to declare an “all clear”? Operations are not *normal* at this point, they are just restored enough to enable critical functionality. This point in the recovery process must be defined in the disaster recovery plan. A person with enough knowledge of the recovery process and business operations should be appointed and given the responsibility to declare an end to the disaster.

Reconstitution Process

As we know from the previous stage of the disaster recovery process, operations have been restored (critical operations anyway). This does not mean that the recovery process is complete. Operations may have been restored at a remote data center, or operations may have been restored using reserve systems. No matter how operations have been restored, they need to be brought back into the first (and sixth) stage of the recovery process, *Normal Operations*.

The reconstitution process restores the operations back to a state that is as close to the original state (prior to the disaster event) as possible, or better. The state in which the reconstitution phase returns operations becomes the new *normal operations* stage.

Normal Operations

The five other stages of the disaster recovery cycle bring us back to the beginning. At stage six, be sure to update your disaster recovery plan with the “new” normal operations and lessons learned through the recovery processes.

Best Practice #2: Engage the Business

We often find disaster recovery planning under the responsibility of information security personnel and we often find information security under the responsibility of IT. Although this may work well for some companies, it is important to stress that disaster recovery is NOT an IT issue. Disaster recovery IS a business issue. Personnel responsible for disaster recovery planning must reach out to all business units within an organization in order to gain an understanding of how systems, applications, information, and facilities are used.

10 Disaster Recovery Best Practices

The most valuable work we do is not done behind a desk or computer.

Senior Management Sign-off and Funding

Disaster recovery planning and/or the lack thereof, have a significant impact on a business. As with anything that has a significant impact on business, senior management sponsorship is critical. Failure to obtain documented senior management sign-off for a disaster recovery planning project will often lead to complete failure or worse yet, you looking for new work.

There are numerous ways to obtain management sign-off and funding, just make sure it is documented.

Planning Group

Nobody knows the value of information resources more than the users who use them. In order to gain an intimate understanding of how information resources (applications, servers, data, etc.), you must reach out to users. The establishment of a disaster recovery planning group is critical to the success of disaster recovery planning because it:

- Enables communication to and from the business
- Fosters cooperation and buy-in
- Allows for shared and delegated responsibility

More than once, we have witnessed a single person attempt to write and implement a disaster recovery plan without the proper input from the business. These disaster recovery plans were all poorly written and ineffective in practice.

Business Impact Analysis

A business impact analysis is used in an attempt to determine how critical a specific information resource (application, server, data, etc.) is to the organization. At the end of a good business impact analysis exercise, the following questions should be answered for each identified information resource:

- How much money would be lost if the information resource were unavailable for one hour? Two hours? One day? One week? Indefinitely?
- How many people are dependent upon the information resource in order to complete job-related tasks?
- How long can this information resource be unavailable before significant damage is done to the company (essentially RTO)?
- How are information resources used to satisfy business requirements?
- What is the peak usage time for a business resource?
- Does this information resource or supporting business function generate revenue for the organization?

There are many more questions that a good business impact analysis can answer. The answers can usually be fed directly into the disaster recovery plan. See [NIST IT Contingency Planning Guide](#) for more information regarding business impact analysis.

A few words of advice if you decide to conduct your business impact analysis through questionnaires; be sure to validate the answers. People have a tendency to rate their systems as more critical than they actually are.

10 Disaster Recovery Best Practices

Best Practice #3: Define the Scope and Objectives

A disaster recovery plan does not necessarily have to take every scenario and every business process and every network device and every person and every application, etc. into consideration. A disaster recovery plan can be scoped down into something that is more manageable for an organization. Some disaster recovery plans only take critical business systems and processes into account. Some disaster recovery plans are IT-centric and only account for IT systems. One scope is no more valid than the other as long as it satisfies the needs of the business.

Be sure to define, and document the scope and objectives of your disaster recovery plan. If you are unsure of the scope, seek the guidance of senior management and your disaster recovery planning group (See Best Practice #2).

Conduct Comprehensive Inventory

Your company should already have a comprehensive inventory of all information resources (applications, servers, data, etc.). If your company does not have a comprehensive inventory, or if the inventory is not up-to-date, this is a perfect opportunity to do one, or update one. There is just no way to know how to restore an environment that isn't well understood to begin with. The inventory should be updated as changes occur and reconciled on a regular basis.

Include a comprehensive information resource inventory in your disaster recovery plan.

Establish Priorities

Some systems are more critical to business operations than are others. With a comprehensive information resource inventory and business impact analysis in hand, you should be well on your way to establishing a solid restoration prioritization schedule. Document the priorities, with specific recovery time objectives (RTOs) and include them in the disaster recovery plan.

Best Practice #4: Understand Systems and Dependencies

Rarely does an information resource operate independent of another. An application may be dependent upon a specific server front-end and another server as a back-end, all dependent on a network architecture for operation. Understanding, documenting, and communicating system dependencies is critical to the restoration of services.

Best Practice #5: Offsite Data Storage

This one seems obvious, but you would be surprised by how many times we run across a company that fails to get this one right. We have seen companies store backup data onsite, in a single site company. We have seen companies store backup data across the street from the single, primary site. Backup data stored at the site that suffers a disaster event usually does little to help the company restore data at a secondary site.

Store backup data far enough from the protected site so that a disaster affecting the protected site will likely not affect the storage site. The distance can vary, depending upon the types of disasters you are trying to protect against and the types of protection offered by the storage site.

10 Disaster Recovery Best Practices

Typically there is a trade-off when it comes to distance. Longer distance might mean better protection, but could also mean delayed restoration.

Offsite data storage can come in the form of backup media (such as tapes), or online. Weigh all of the options before deciding on the best approach for your business.

Best Practice #6: Don't Forget Support Data

Operational data is not the only data of critical importance to an organization. Log files, configuration files, passwords, encryption keys, etc. could also be of critical importance. Don't forget to address these other data types in your disaster recovery plan. The wrong time to not have an encryption key is when you need to decrypt data during a restoration!

Best Practice #7: Update Continuously

A disaster recovery plan is a point-in-time plan to recover information processing. An outdated disaster recovery plan can be dangerous in that it won't allow for an effective recovery, which could in turn lead to a loss of critical data and/or an extended period of disrupted business operation. As applications, servers, data, business processes, etc. change, so must your disaster recovery plan.

Integrate updates to the disaster recovery plan with change control. This should ensure that changes to the environment are reflected in the disaster recovery plan. Additionally, the disaster recovery plan should be reviewed no less than annually.

Best Practice #8: Use Checklists

People don't like to read when they are under pressure or in a high-stress situation. A disaster recovery can be emotionally draining and the pressure to restore systems as soon as possible can be overwhelming. The last thing you want to do is to stop and search for information within paragraphs and chapters of information. Make things as easy-to-follow as possible, and use checklists everywhere. Checklists make reference a snap and reduce errors.

Best Practice #9: Test, Test, and Test

There are only two ways to make sure that your disaster recovery plan works as intended; test it thoroughly or suffer a disaster. The right time to find out that your disaster recovery plan needs work is during testing, the wrong time to find out is during a disaster. Test the plan until you get it right, and then test the plan annually thereafter.

Be sure that your testing doesn't disrupt the business and cause a disaster itself!

10 Disaster Recovery Best Practices

Best Practice #10: Store Plans Offsite

See Best Practice #5. A disaster recovery plan stored only at the site suffering a disaster does little good to recover the site. It is risky to not store disaster recovery plans offsite where they can be made readily available in the event of a disaster.

Bonus Best Practice: Don't Forget about Security

A disaster recovery plan that does not take information security into account could easily end up suffering another disaster soon after recovering from the first one. The restored site must have the same (or better) information security controls than did the original. Some companies even go so far as to perform an information security assessment on the recovery site immediately following restoration of operations. A poorly secured restoration is dangerous.

About FRSecure

FRSecure LLC is a full-service information security consulting company dedicated to information security education, awareness, application, and improvement. FRSecure works with businesses of all sizes, in all industries; enabling clients to achieve optimal results per information security dollar spent. Every one of our clients is in business to make money, so we design secure solutions that drive business, protect sensitive information assets, and improve the bottom line.

Regulatory and industry compliance is built into our solutions. Our experience has shown that good information security equals compliance, not the other way around.

To read more about FRSecure, visit us online at <http://www.frsecure.com>.