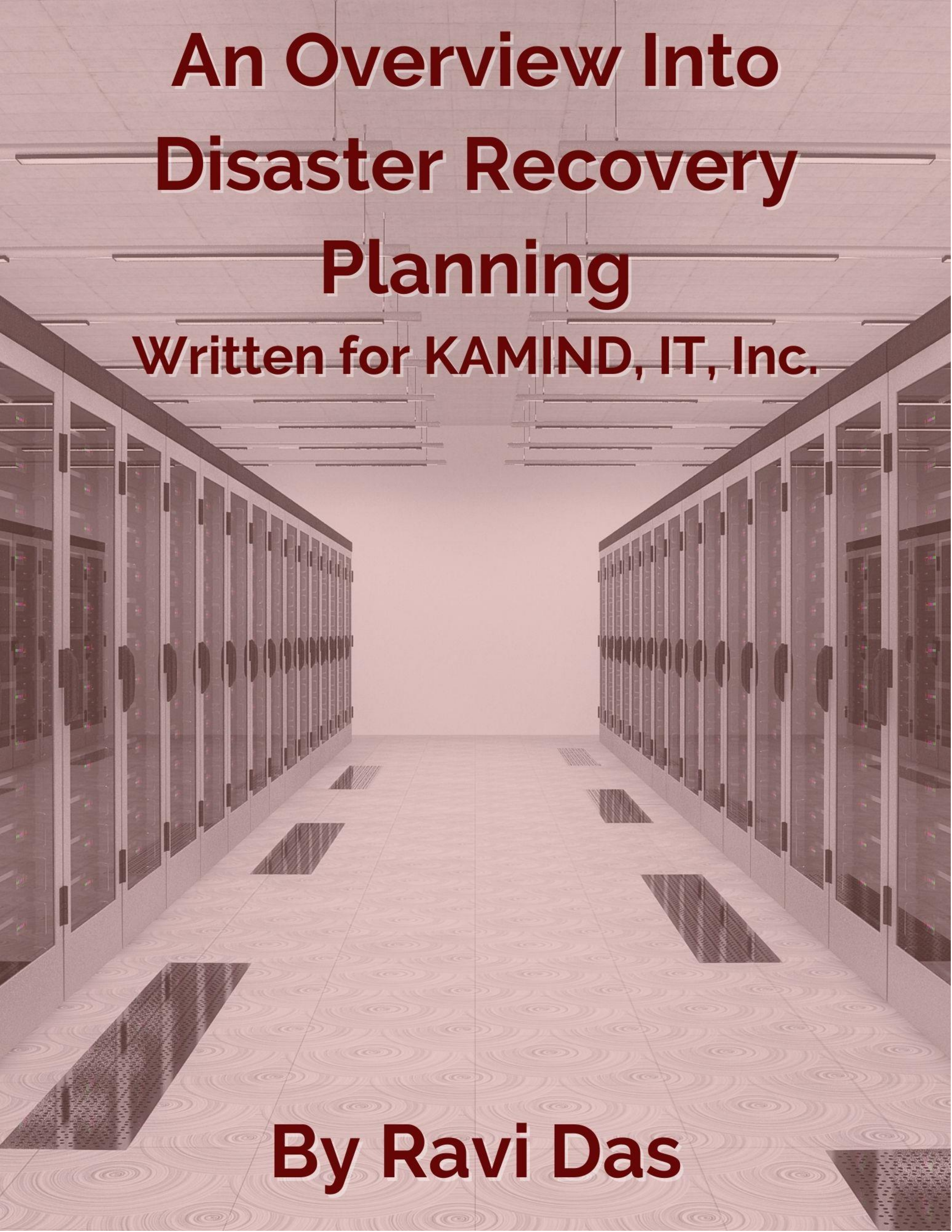
An Overview Into Disaster Recovery Planning

Written for KAMIND, IT, Inc.



By Ravi Das

Introduction

This is a business owner's worst nightmare: Everything seems to be going well for a long period of time, and then all of a sudden, a disaster strikes, impacting your operations, your employees, and your customers. But given just how interconnected everything is today, there are also indirect parties that are all impacted as well, which include your suppliers and distributors, shareholders, families, contractors, any external third parties that you may outsource work to, your advisory board, and even the board of directors.

Depending upon the magnitude of the disaster, it could take a very long time to recover, and the need to come back to life as quickly as possible is of course of the utmost importance. But how does one go about this? This is of course no easy task to accomplish, but the process all begins with a very carefully crafted plan that can be launched and executed in just a matter of minutes.

This is where the role of a Disaster Recovery plan comes into place, as it spells out the exact process of what needs to be done in order to bring up at least the mission critical operations, then from there, the other processes that need to be redeployed.

Given the Cyberthreat Landscape of today, this plan is becoming even more vital by the day. For instance, one just never knows when they will become the victim of the next Cyberattacker, no matter how large or small it is. But given the sheer importance of Disaster Recovery planning, many businesses and corporations are simply not understanding the magnitude of the potential dangers that they face.

Consider some of these statistics:

- 58% of businesses are not handled to prepared data loss when disaster strikes;
- 60% of the SMBs that actually lose information and data will be forced to shut within a 6-month time span;
- There are over 140,000 hard drive failures in SMBs on a weekly basis without any plan in place in recovering the lost information and data;
- Almost 30% of hard drive failures are caused by some sort of disaster, whether it is natural or Cyber-related.

(SOURCE: 1).

It is important to keep in mind that creating a Disaster Recovery Plan can be a complex process as well as a huge undertaking. There is no cookie cutter approach in doing this, a lot depends upon the requirements of your own business. The goal of this whitepaper is to introduce you to the overall concept of a Disaster Recovery Plan. A subsequent whitepaper will examine in much further detail as to how you should go about creating and executing such a plan.

The Importance of a Disaster Recovery Plan

<u>The Definition of a Disaster Recovery Plan</u>

When one thinks of a disaster, the first thought that comes to mind is a Cyberattack, ranging anywhere from Ransomware, to Phishing, to Trojan Horses/Malware/Spyware to even Social Engineering. While this is the trend these days, a disaster can also include anything natural as well, such as a tornado, hurricane, or even a massive thunderstorm. The bottom line is that if your business is impacted in such a way that it needs to shut down in order to recover and bring up the mission critical operations, you have been hit by a disaster. The question that is often thought of first is, "What exactly is a Disaster Recovery Plan"? It can be defined specifically as follows:

"A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster. Disaster recovery planning is just part of business continuity planning and applied to aspects of an organization that rely on an IT infrastructure to function.

The overall idea is to develop a plan that will allow the IT department to recover enough data and system functionality to allow a business or organization to operate - even possibly at a minimal level."

(SOURCE: 2).

Based from the definition above, a Disaster Recovery Plan is just that – it is a comprehensive document or even a set of documents that lays out the needed steps in order to bring your business back up to the base level that is needed in order to conduct transactions and meet the immediate needs of customers. In fact, Disaster Recovery Planning is just one part of a triad that needs to be taken into consideration when impacted.

The other two areas are:

- <u>The Incident Response Plan</u>:

  This details as to how your business or corporation will respond to a disaster and mitigate any damage that is caused from it.

- <u>The Business Continuity Plan</u>:

  This is also further details as to how you will restore business operations for the longer term, after you have restored mission critical operations (which is the goal of the Disaster Recovery Plan). In other words, this plan will bring your organization back up to speed to the point where it operated normally just before the disaster hit.

<u>The Categories of Disaster</u>

In creating your Disaster Recovery Plan, there are three levels of Disaster that you need to be aware of, and are as follows:

1) <u>Minor Disasters</u>:

   These are the kinds of disasters which inflict just a minor financial damage to the business or corporation. For instance, it could be just a worm that has penetrated your IT Infrastructure and has not really caused much of an impact other than just being a sheer nuisance or annoyance.

2) <u>Major Disasters</u>:

   This is the type of disaster where a major portion of your IT Infrastructure has been hit, impacting everything from the servers to the workstations and all types of wireless devices. Also, a huge amount of sensitive and proprietary customer information/data has been stolen or covertly hijacked. Your IT Department and parts of your business simply cannot function in a normal fashion, and for all intents and purposes, they will have to be shut down. This is the kind of Cyberattack that most organizations are experiencing today.

3) Catastrophic Disasters:

This is the worst kind of disaster. In this kind of situation, the costs of restoring business operations far outweigh the benefits, and as a result, the organization will just have to simply shut down permanently. So far, this magnitude of Cyberattack has not happened on a large scale yet but given the sophistication level of the Cyberattacker these days, it is bound to happen sooner or later.

The Benefits of a Disaster Recovery Plan

Apart from restoring your mission critical processes up in a short of period of time, a well-documented Disaster Recovery Plan has other numerous benefits as well, which include the following:

1) Your organization will achieve greater cost efficiencies:

For example, before you can even engage in creating a Disaster Recovery Plan, you must first complete what is known as a "Business Impact Analysis", also known as a "BIA" for short. It is defined as:

"A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions and plans."

(SOURCE: 3).

In other words, you are mapping out those IT assets that are at risk if and when a Cyberattack actually occurs and quantifying that level of risk. From there, they will then be categorized such as:

- High Risk;
- Medium Risk;
- Low Risk.

By ascertaining this, you and your IT Security team will know which and how much of resources need to be dedicated to protecting those IT Assets that are at most risk, thus resulting in an efficient spend of a tight IT budget.

2) An increased level in worker productivity:

Believe it or not, a good Disaster Recovery Plan can actually improve the morale of your workforce, which will in turn increase their productivity levels. For example, when creating it, you will be assigning your employees various tasks that they must do in the face of a Cyberattack. Knowing that they are making a positive impact in this fashion will only strengthen their belief that they are actually contributing to a greater good of the company, other than simply doing their daily job tasks.

3) A happier customer base:

Because of all of the new Cyberthreats that are coming out, as well as their variants, customers are becoming much more cautious in regard to opening any emails that they receive, the links they click on, and even the websites that they visit. For example, although Phishing remains one of the oldest attack vectors that is in existence, many Cyberattackers are still using it in order to covertly hijack the Personal Identifiable Information (PII) of unsuspecting victims. In other words, your customers want to know that they as a business owner, that you are taking every precaution possible to protect their respective PIIs. By demonstrating to them that you have a solidified Disaster Recovery Plan in place, this will only bolster their confidence to stay with you as customers and bring in repeat business. It means that they feel safe and comforted knowing that in the unfortunate chance you are impacted by a Cybersecurity attack, there are plans in plans in place so that their PII will not, as far as possible, fall into the hands of a Cyberattacker.

4) You will have a better sense of scalability:

After completing your Business Impact Analysis (BIA) as previously described, you and your IT Security team will have a much greater understanding of the types of resources that will be needed to protect them. Some of these resources will be either based On Premises, or in the Cloud, or perhaps even a combination of both. Having such resources with the latter will offer your organization a much greater realization of scalability. For example, you can ramp up or ramp down very quickly those resources, when an IT Asset changes a risk category. For example, if a "High Risk" asset becomes downgraded to a "Medium Risk" categorization, those resources that were dedicated before can be scaled down to meet the new requirements very quickly. This will also help your organization in realizing greater cost efficiencies as well.

The Types of Disaster Recovery Plans

As mentioned before in this whitepaper, there is no "one size fits all" Disaster Recovery (DR) Plan. Much of the details that go into it will depend upon your own security requirements and needs. With that in mind, there is yet another very important consideration that you need to factor in creating your DR; and that is the kind of facility you want to use to restore your mission critical operations, and eventually, your entire business.

There are a number of types of them, and they are as follows:

1) A Cold Site Facility:

This is where you rent out a secondary, physical office location in which you can start to reestablish your business after you have been impacted by a Cyberattack. These kinds of providers offer the tools that you need to get your servers up and running, which includes the proper levels of electrical power, cooling, and network connectivity. But, keep in mind that this kind of facility is bare bones in nature in that you will have to install the new hardware, reinstall any existing software applications as well as your databases, and even uploading your information and data once again from the backup tapes that you have used. As a result, this kind of approach can take a much longer time to restore critical business operations. Therefore, this option, while it is inexpensive from the outset, the costs can add up very quickly in just a short period of time.

2) A Hot Site Facility:

This is actually the opposite of the Cold Site Facility, as just previously described. In this kind of scenario, the secondary office location is an exact replica of your existing IT Infrastructure that you already have in place in your current business facility. This means that this facility is completely set up for you with regards to all of the software, hardware, and network connectivity that you will need to be up and running with crucial operations in just a matter of a couple of hours. This kind of set up even comes with all of the communications you will need in order to reach out to your teams between the Hot Site Facility and your existing place of business, including all of the wireless devices you will need, and even full time technical support. In fact, all of your databases are also replicated at this facility, so reloading information and data is not even an issue. With a Hot Site Facility, it is just like you walked into a new office setting as if nothing ever happened. While the primary advantage of this is that there is virtually no downtime experienced in restoring operations, the main disadvantage is that this kind of set up can be extremely costly to a business.

3) The Cloud Infrastructure:

In this kind of Disaster Recovery setup, you have your entire IT Infrastructure outsourced to a Cloud Provider. In fact, this can be considered just like a Hot Site Facility but rather than having a physical facility, it is all virtual, literally in the Cloud. One of the key advantages of this is that you do not have to bear responsibility for any kind of hardware or software upgrades or licensing issues, it is all up to the Cloud Provider to do this for you. Also, they are responsible for keeping backups of all of the information and data that you have stored with them, as well as ensuring the latest security protocols have been implemented onto your Virtual Servers (also known as "Virtual Machines"). This kind of setup makes it that much easier to actually conduct a Disaster Recovery drill. These Virtual Machines can be replicated anywhere in just a matter of a few seconds, so even creating backups of these should not be a problem. But best of all, the price is extremely affordable for any business: It is fixed and can be paid on a monthly basis. When in comparison to a Cold Site or a Hot Site Facility, the costs of a Cloud Infrastructure are very nominal.

The Components of a Disaster Recovery Plan

There are many important items to a Disaster Recovery Plan, and each will have to be tailored to meet the needs of your business and requirements. In this section, we outline some of the key aspects that you should include in it:

1) Create the Disaster Recovery Team:

This is probably deemed to be one of the most crucial aspects of the Disaster Recovery Plan. This will be the team of your employees that will be responsible for acting on their own areas in order to bring the business back up and running as quickly as possible after you have been hit by a Cyberattack. This area should clearly detail the following:

- ➢ The team members who will be part of the actual Disaster Recovery Team;
- ➢ Their specific responsibilities;
- ➢ Most importantly, their contact information. This should include work phone number, work Email address, home phone number, and even personal Email address as well. Also, make sure to include all cell phone numbers as well, even both work and personal.

It is important to note the team members should include representatives from all of the departments that you may have. Depending upon how large the business is, upper management and even the C-Suite should also be included as well. Remember, clear and concise communications amongst all of the team members here, as any time wasted will only translate into further downtime, which could be detrimental in the end. Also, make sure that all contact information is up to date as well.

2) Moving your equipment:

Depending upon the kind of Disaster Recovery setup you choose to establish (as reviewed in the last section), the Disaster Recovery Plan needs to have a component as to how all of the employee related equipment will be moved. Although your IT Infrastructure will be replicated in a Cloud Infrastructure or at the secondary physical site, there are still things that have to be immediately transitioned over, in order for your employees to bring your business back up to a normal state of operations once again. This includes all workstations, computers, and wireless devices that are used to conduct everyday job functions. In this regard, it is also wise to make advanced plans with a moving company that specializes in Disaster Recovery so that items can be moved very quickly. In this regard, your Disaster Recovery Team should also keep an active inventory of all of these items, and make sure that it is always updated.

3) Business Continuity:

Another plan that must be created in conjunction with the Disaster Recovery Plan is the Business Continuity Plan. This document or set of documents should specifically detail how the business will continue to keep running in a normal state once the mission critical processes are back up and fully operational. By compiling this Plan, you will get a solid understanding as well as to how the business truly functions and operates. As a result of this, you and your Disaster Recovery Team will know exactly what operations and processes need to be brought up again in their order of relevant importance. Keep in mind that while the Business Continuity Plan is actually a separate entity, the major highlights of it should be include here, in the Disaster Recovery Plan.

4) Daily checks on the Data Backups:

Although the backup databases and the confidential information and data they contain will either reside in a Cloud Infrastructure or at a physical off-site location, it is very important that they are tested on a regular basis to make sure that they are still working at optimal conditions, and will be ready to be deployed and go into action in the aftermath of a Cyberattack. Equally critical is that they are also updated with the latest software upgrades and patches, and that they reflect the most recent copies of your primary databases. In other words, whatever procedures you carry out on the primary databases should also be carried out onto the backup databases, preferably on the same day, so that everything remains as current as possible, and in a constant of readiness.

5) Restoring operations with the Vendors:

Apart from bringing back up your operations to a normal state once again, it is also equally important to have a part in the Disaster Recovery Plan that outlines how you will restore communications and processes with your suppliers and vendors. The bottom line is that any downtime lost in the production of goods and services will only result in lost customers in a very short period of time. Therefore, you will need to work out some sort of system with your external third parties in order to make sure that the needed parts, components, and supplies will be fully stocked once you are ready to resume back to a production status once again.

6) Document Recovery:

Apart from the Intellectual Property (IP) that your business may have, another key asset that your business possesses are all of the documents that it possesses. This can range anywhere from employee records to financial statements to even internal user manuals. Therefore, it is very imperative that these are backed up as well, in line with the same manner as it has been detailed with the data backups. In this scenario, you may even want to contract out this kind of service to a well reputed Document Restoration company, who will be able to help your Disaster Recovery Team to bring back all documentation online after mission critical operations have deemed to be fully functional.

Conclusions

Overall, this whitepaper has examined the importance of having a Disaster Recovery Plan, the various types of them, and what should be included. But it is very crucial to remember that this Plan is not static by any means. In other words, once it is created and implemented it must be rehearsed at minimum once a quarter so that your Team knows exactly what they need to do in the face of a Cyberattack. Also, by practicing it, you will be able to determine where the gaps and weaknesses lie at, and thus your Plan to can be appropriately tweaked as such.

Another option for you to consider for your business is what is known as “Disaster Recovery as a Service”, also known as “DRaaS”. This is where you outsource your entire Disaster Recovery function to an entrusted, third party to do all of the planning and work for you. This will be the focal point of the next whitepaper in this series.

Sources

1) https://smallbiztrends.com/2017/04/not-prepared-for-data-loss.html
2) https://www.techopedia.com/definition/1074/disaster-recovery-plan-drp
3) https://www.gartner.com/it-glossary/bia-business-impact-analysis
4) https://www.codero.com/resources/blog/5-key-elements-business-continuity-and-disaster-recovery-plan/
5) https://www.evolveip.net/blog/4-benefits-disaster-recovery-planning
6) https://www.empowerit.com.au/blog/it-planning/different-types-disaster-recovery-plans/
7) https://entechus.com/7-key-elements-of-a-business-disaster-recovery-plan/

8) https://www.polygongroup.com/en-US/blog/top-5-components-of-the-best-business-disaster-recovery-plans/

9) https://blog.itfreedom.com/blog/importance-of-a-disaster-recovery-plan