

Disaster Recovery Simplified

by

Mitchell Stehlin & Matthew Lehrian

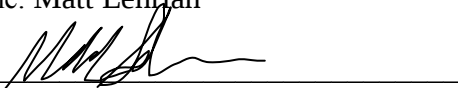
Submitted to
The Faculty of the School of Information Technology
In Partial Fulfillment of the Requirements for
The Degree of Bachelor of Science
In Information Technology

© Copyright 2016 Mitchell Stehlin, Matthew Lehrian

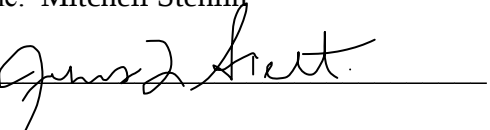
The author grants to the School of Information Technology permission
to reproduce and distribute copies of this document in whole or in part.

Learner's signature:  Date: 4-18-16

Learner's printed name: Matt Lehrian

Learner's signature:  Date: 4-18-16

Learner's printed name: Mitchell Stehlin

Advisor's signature:  Date: 4.18.16

Advisor's printed name: James Scott

University of Cincinnati
College of Education, Criminal Justice, and Human Services
Spring 2016

CONTENTS

CONTENTS.....	i
LIST OF ILLUSTRATIONS.....	ii
ABSTRACT.....	1
INTRODUCTION	2
PROBLEM.....	2
SOLUTION.....	2
PROJECT GOALS	3
OVERVIEW	3
DISCUSSION	4
CONCEPT	4
CONSTRAINTS	7
RISKS	9
TECHNICAL ELEMENTS	11
REQUIREMENTS.....	11
TESTING	11
SCENARIOS	12
PROPOSED BUDGET.....	15
CONCLUSION.....	17
NOTES.....	18
BIBLIOGRAPHY	19

LIST OF ILLUSTRATIONS

Figure 1: Hardware Topology.....	4
Figure 2: User Profile.....	7
Figure 3: Causes of Downtime	9
Table 1: Testing Criteria	12
Figure 4: Scenario B Logical Diagram	14
Table 2: Scenario A Budget	15
Table 3: Scenario B Budget	16
Table 4: Scenario C Budget	16
Table 5: Project Budget	16

ABSTRACT

A service with 99% availability is still down for 87.6 hours a year. When one day of downtime costs most small and medium sized businesses \$12,500 or more;¹ backup and recovery systems are imperative. While natural disasters must be planned for, many system outages are caused by people and processes. Even for small and medium sized business (SMB) owners, system outages pose a significant risk. With the line blurring between which IT systems are business critical and which are not, the need for backup systems increases. The key to any disaster recovery (DR) solution is proper risk evaluation and requirement drafting. However, budgets are the main constraint for any company. Cost-effective and simple DR solutions are needed, as expertise and budgets can be limited for companies new to DR. Of course, risks, requirements, and budgets will vary; which is why this project presents effective and budget-conscious disaster recovery solutions.

INTRODUCTION

PROBLEM

The context of this project focuses on businesses and their ability to recover IT systems from unexpected outages or disasters. The target audience will be smaller and medium sized businesses (SMB's) that struggle with disaster recovery (DR). Almost every business these days utilizes IT systems that run business critical applications and store sensitive data. Several constraints exist when it comes to the information technology aspect of business continuity. These constraints include evaluating risks, assessing requirements, and testing DR solutions. Other major hurdles for companies are a lack of time, money, and expertise. Common DR solution providers have trouble scaling down to the needs of smaller, more agile companies. Finally, disasters are not exactly the only concern. After all, 80% of unplanned outages are caused by procedural and human error.³

SOLUTION

The proposed solution to these problems is DR planning tailored for small and medium sized businesses. This project aims to showcase DR demonstrations that focus on common constraints of SMB's. Another goal of the project is to make the assessment of risks and requirements easier for business owners or IT managers. Technical demonstrations and visualizations will be created to showcase what a realistic disaster recovery solution could look like for different business scenarios. The demo will also present important concepts that must be considered when planning for system outages and disasters. The solution will employ virtualization, cloud technology, and sensible planning to make disaster recovery a reality for small to medium sized businesses. The goal of this project is to clear up misconceptions and confusion around disaster recovery concepts

and solutions. Business owners and system administrators will be able to use this project as reference material when planning and implementing their own solutions.

PROJECT GOALS

There are four goals that this project aims to achieve. The first goal is to help business owners and IT administrators understand risks associated with the downtime of IT systems. There is much more to disaster recovery than just avoiding a natural disaster. The second goal is to guide business owners and IT administrators on the assessment and creation of requirements. Solutions for DR need to take into account the recovery point objective, recovery time objective, maximum tolerable downtime, and several other factors. Goal number three is to describe technical components, constraints, and considerations for DR solutions. This will help stakeholders get a clear idea of what technology can be involved with DR. Lastly, the fourth goal is to showcase technical demonstrations of disaster recovery solutions. This is intended to help administrators and stakeholders understand exactly what a DR solution could look like and how it could work for their company.

OVERVIEW

Business continuity and contingency planning must be taken into consideration for all businesses. The problem is, half of small to medium sized businesses do not have a plan in place to recover from unplanned outages³. Business owners and system administrators often underestimate the risks of outages. Even though natural disasters and severe weather events are relatively uncommon, outages are largely caused by human error. Furthermore, it is difficult for businesses to find the time, money, and expertise to solve this problem. The proposed solution to this problem is a report

that helps stakeholders understand the assessment of risks and requirements, while showcasing DR concepts and technical solutions. The main goals of the project are to introduce risks that need to be considered, outline requirements for DR solutions, describe the necessary technology involved, and provide a technical demonstration of a disaster recovery solution.

DISCUSSION

CONCEPT

The concept of this project is to assist small and medium sized businesses who do not have a DR plan. Furthermore, this project can be of use to businesses who may have a partial DR plan but need help solidifying it. Cost analysis and simplicity will be major focuses because the target audience is often limited by budget and expertise. Solutions for DR will be simulated and demonstrated on hardware maintained by the team. Figure 1 shows a diagram of the topology and equipment involved with part of the technical aspect of this project. Network attached storage will be used to power two separate sites. The desktop PC will act as the main datacenter and the Dell PowerEdge will act as the DR datacenter.

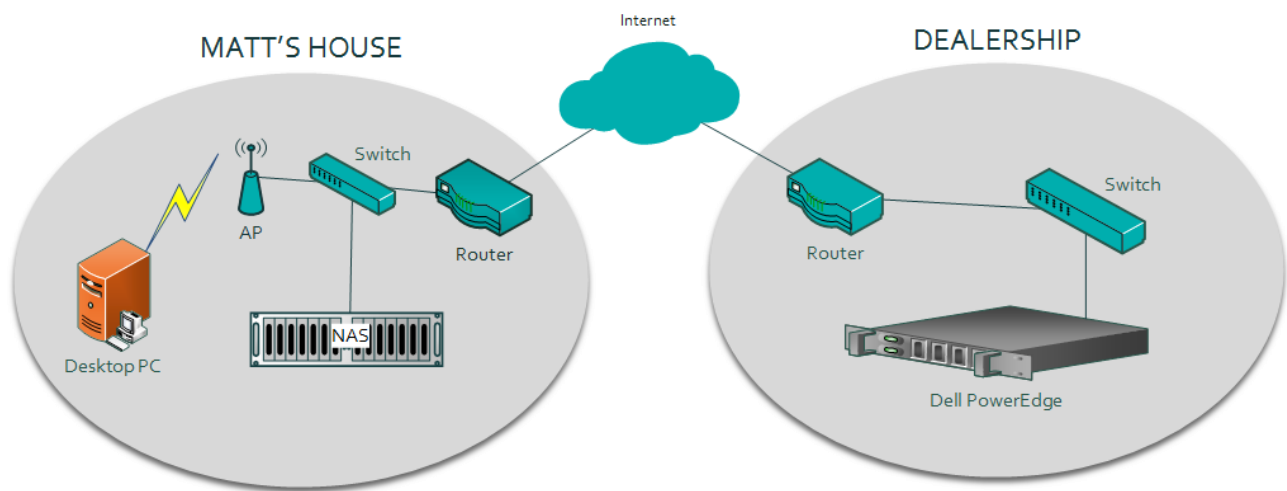


Figure 1: Hardware Topology

USER PROFILE

Figure 2 below introduces our user profile.

PROJECT: Disaster Recovery Simplified
POTENTIAL USERS: - Infrastructure/Operations system administrator - Small to medium sized business owners - Business continuity staff
SOFTWARE, INTERFACE, AND RELATED EXPERIENCE: This project will partially be aimed at non-technical business owners and business continuity personnel. These users will likely have experience with common operating systems, e-mail clients, and web browsers. While they are not necessarily technical, their experience with common software will allow them to follow along with the demonstration and benefit from the concepts introduced. Business owners may have experience with recovery solutions. Business continuity personnel will have experience with recovery solutions that focus on business operations and not necessarily IT operations of the company. They can leverage this experience to learn and become effective with regard to the IT component of business continuity. The other portion of users being profiled are system administrators in various capacities. These are people who manage computer systems at small to medium sized businesses. They most likely have experience with several of the following: - Server operating systems - Network device configuration pages - Database and storage solutions - Hardware acquisition/operation/maintenance

- IT facilities
- Environmental and connectivity factors

EXPERIENCE WITH SIMILAR APPLICATIONS:

Business owners and business continuity personnel are not likely to have experience with the processes and applications being showcased in the demonstration. However, they will understand concepts and better understand the disaster recovery process.

System administrators may have experience with the same or similar applications that will be used in the demo. This includes databases, server and network configuration, and possibly virtualization software.

TASK EXPERIENCE:

Business owners will have experience with various tasks related to business operation and management. This may or may not include firsthand experience with IT. In some cases, the business owner is the system administrator. Task experience will vary, but at a minimum the business owner will have experience with ensuring the proper operation of business critical IT systems.

Business continuity personnel are usually tasked with keeping the business operational through unforeseen and adverse events. These events could include severe weather, power outages, and system failures. They design plans and procedures to follow when various events occur. Plans usually include specific instructions on how to resume business operations, employee roles, and relocation.

Finally, system administrators have experience with most IT operations for small to medium sized businesses. This includes managing IT infrastructure, business applications, company e-mail, desktop environments, data storage, backups, and other common system

admin roles. Some may have experience with virtualization and other more advanced systems.
FREQUENCY OF USE: The actual project and demonstration will basically be a one-time use. However, the solution we are providing can be used by companies whenever the need calls for it. If things go well, disaster recovery solutions should only be used monthly for testing. In the event of a disaster, the solution should seamlessly transfer operations from the main data center to the recovery data center.
KEY PROJECT DESIGN REQUIREMENTS THAT THE PROFILE SUGGESTS: - Adaptation for business owners and business continuity personnel - Technical information and demonstration of disaster recovery solution. - Overview of requirement and risk assessment - Engaging presentation - Visually and aesthetically pleasing designs - Images that inform and enhance the presentation

Figure 2: User Profile

CONSTRAINTS

This problem has many variables that need to be taken into consideration. First and foremost, is the business owners and IT admins. Often times they underestimate the risks posed by a system outage. This problem is exasperated by the fact that businesses in the information age require increasing uptime for customer services. Many small to medium sized businesses do not make disaster recovery a priority. Even though a severe outage would threaten the livelihood of the business, backup and recovery are an afterthought.

Second, businesses are often limited by resources. Time, money, and labor are all hard to come by in a small to medium sized business. Therefore, many disaster recovery solutions end up being incomplete and insufficient. Stakeholders are not always aware of various concepts surrounding DR. Informational material about disaster recovery is usually either too dense or too brief. Executives and IT admins need help creating and visualizing solutions for DR.

Another aspect of this problem is the testing of recovery systems. Just because a company has backup systems does not mean they have an effective DR solution. Recovery relies on planning and testing. A plan must be in place for the resumption of both IT and business operations. However, without regular testing, all of the recovery plans could be useless. The typical recommendation is to test backup plans and systems about once a month.

Lastly, other problems come up depending on the characteristics of the business. Sometimes the business owner and the IT manager are the same person. Businesses do not always have highly capable IT staff. This poses a problem because there might not be anyone in the business that is experienced with creating and implementing a comprehensive DR solution.

RISKS

The risks of disasters, outages, and downtime can be hard to convey to small and medium sized businesses. It is important to note that outages and downtime are not only a result of severe weather events. Hardware failure, software failure, and human error account for 95% of downtime.⁴ Hardware failure actually accounted for the largest percent of disasters. It may seem unlikely; as most hardware has several redundant components. But still, one can never predict when hardware is going to fail and it is important to consider this type of disaster. Software failure and human error are also significant risks that are often underestimated. That routine patch or update could cause a nasty interaction that brings on a full scale outage. Also, humans are not perfect, and accidents happen. Simple mistakes can sometimes lead to significant outages. These are all risks that must be taken into consideration with any disaster recovery plan.

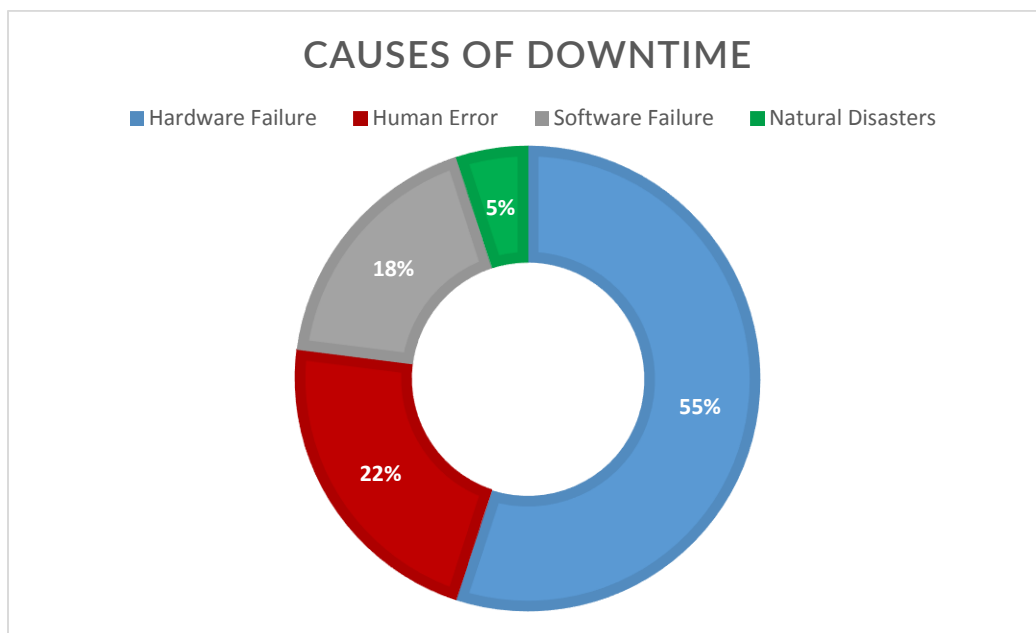


Figure 3: Causes of Downtime

REQUIREMENTS

An effective DR solution will have several different requirements that will vary between different companies. The two major concepts to consider for a recovery solution are the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO). The RPO is the amount of data loss a business can survive, measured in time. For example, if backups are run every Friday, and systems go down on a Thursday, four business days' worth of data could be lost. The RTO refers to the amount of time that passes from the point of a complete system outage, to the point of the recovery systems going live. RTO also depends on the Maximum Tolerable Downtime (MTD). The MTD is the amount of downtime that a company can sustain before irreversible damage is caused to the business. Executives from the business and IT side will need to be consulted to formulate the RPO, RTO, and MTD. Once these figures are established, the disaster recovery solution can be constructed to meet the aforementioned criteria.

TECHNICAL ELEMENTS

REQUIREMENTS

Technical and non-technical requirements exist for disaster recovery solutions. The non-technical requirements include RPO, RTO, and MTD. Technical requirements can vary greatly depending on the non-technical requirements. Infrastructure and failover strategies will be decided by the RPO and RTO. Technologies will be selected based on their ability to meet requirements.

PROCEDURES

Failover is the act of transferring IT operations to recovery systems so they can go live after a disaster. Many strategies exist for failover. This is an area where virtualization and cloud technology are extremely beneficial. Failover strategies will determine other procedures such as backup plans and replication. Replication is the procedure of copying production data to recovery systems so data is ready in the event of a failover. Fallback, is the procedure of moving operations from the recovery site back to the main site. Aside from IT related procedures, the business continuity side of DR has several plans to consider. Business continuity is focused not only on the recovery of IT systems, but the resumption of business operations. This can include plans for communication and relocation of employees among other things.

TESTING

A study done by Symantec found that only 28% of small to mid-sized companies have tested their backup.⁴ Disaster recovery plans often fail when proper testing does not occur before hand. Table 1 below shows the criteria we used to test our own solutions.

Stages	Failover			Fallback			
Processes	Simulate Outage	Boot VM's at DR site	Configure Network	Write Data	Migrate to main site	Adjust configurations	Write data
Pass/Fail							

Table 1: Testing Criteria

Ultimately, our testing yielded passing results for all three of our solutions. Of course, we had a number of failures before we got our solutions configured properly. The writing data and simulating outages steps usually passed as they are fairly simple. The rest of the steps were more difficult and took some tweaking. When using these solutions in a production environment, testing needs to be comprehensive and occur about once a month.

SCENARIOS

This report outlines three scenarios that SMB's in the real world might encounter. Prior consulting experience and information from local businesses will be used to determine three different levels of requirements. They will be based mainly on the factors of RPO, RTO, MTD, and budget.

- A. The first scenario accounts for companies who do not need low recovery point and time objectives. These companies usually have low budgets as well. The goal of the scenario will be to construct a low cost and low complexity DR solution for companies with limited time, money, and expertise. Scenario A provides adequate disaster/outage protection for smaller companies. These options do not provide a quick return to operations time, but they still help to keep the business safe from disasters that would otherwise destroy the business.

Companies such as BackBlaze, Carbonite, IDrive, and Mozy all provide small business level backup solutions that will protect from data loss. Cost will depend on storage and compute needs. This scenario uses BackBlaze B2 Cloud Storage with Amazon's EC2 compute service. In the event of a disaster, IT operations will be migrated to EC2 instances and data will be restored from BackBlaze. Automatic backups keep data safe, and the cloud compute instance can be accessed from anywhere. With a strategy similar to this, a severe outage will be manageable for a small business.

- B. This scenario will build on the first one, increasing compute and storage requirements. The goal will be to lower the recovery and time objectives, while staying mindful of the budget. A similar strategy to Scenario A will be used with added capability. This solution utilizes a combination of VMware and Amazon Web Services. Data at the main site will regularly be saved on Amazon's S3 storage. The business will only have to pay to store the data. In the event of an outage, the business will be able to boot virtual machine images using Amazon's EC2 On-Demand compute service. This allows businesses to save money by not running compute or processing in the cloud until they need it. Since storage is relatively cheap, this scenario presents the best value for a budget-friendly DR solution. Figure 4 shown below displays a logical diagram of the AWS and VMware solution.

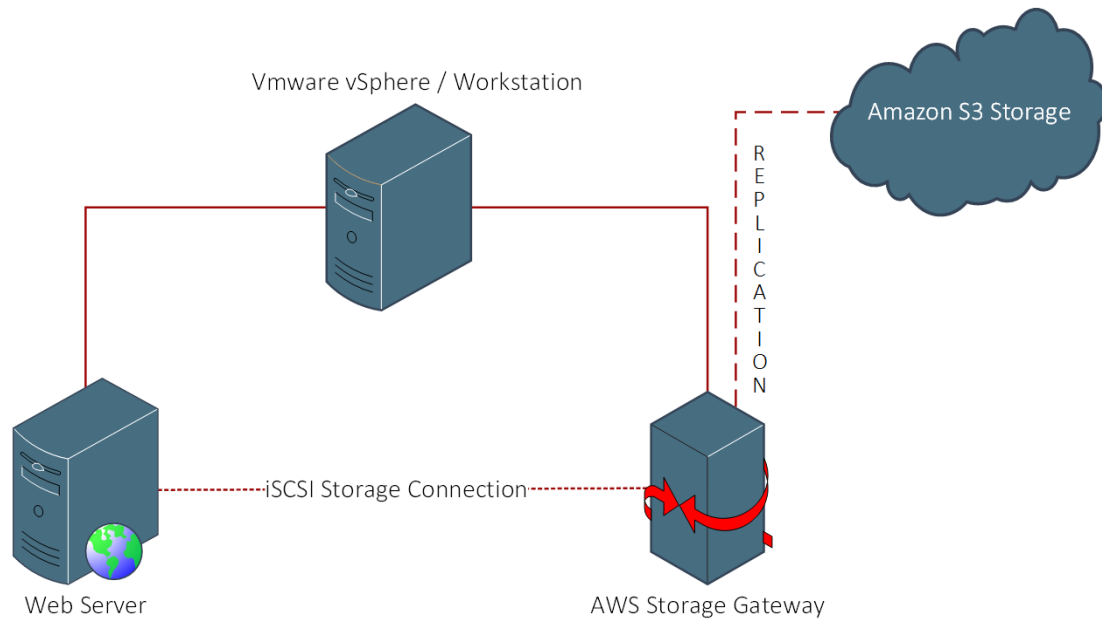


Figure 4: Scenario B Logical Diagram

C. The last scenario is geared more towards mid-sized companies. Recovery point and time objectives are near-zero. This solution uses VMware as the main technology because of the High Availability (HA) feature that allows for near-zero RTO. Figure 4 below shows a logical diagram of how the solution is set up.

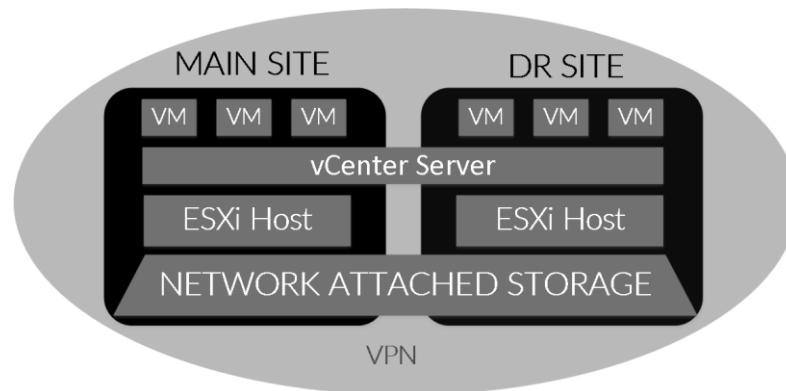


Figure 5: VMware Logical Diagram

The vCenter server is used to control virtual machines (VM's) at both sites. In the event of a disaster, VM's will migrate to the recovery site and continue regular operations.

PROPOSED BUDGET

No money has been spent on the project. However, our hypothetical budgets from our three scenarios are detailed below in Tables 1, 2, and 3. Actual budget is show in Table 4. We were able to keep our actual expenses at \$0 by utilizing free software through the University of Cincinnati and trial accounts with Amazon Web Services.

<u>Scenario A</u>			
<i>ITEM</i>	<i>COST</i>	<i>QUANTITY</i>	<i>TOTAL</i>
BackBlaze B2 Cloud Storage	\$0.005 / GB / Month	500GB	\$2.50 /
	Free Upload	\$2.50 /Month	Month
	\$0.05 / GB Download	\$25.00 (DL)	\$25.00
Amazon EC2 On-Demand t2.medium Instance	\$0.072 / Hour	2 @ 168 Hours (estimated)	\$24.20
Windows 7 Pro	\$51.65	2	\$103.30
			\$127.50

Table 2: Scenario A Budget

Scenario B

ITEM	COST	QUANTITY	TOTAL
Vmware Workstation 12 Pro	\$187.49	1	\$187.49
Windows Server 2012 R2 Standard	\$882.00	1	\$882.00
Choice of Linux distro	\$0.00	2	\$0.00
Amazon EC2 On-Demand t2.large Instance	\$0.104 / Hour	3 @ 168 Hours (estimated)	\$52.41
			\$1,121.90

Table 3: Scenario B Budget

Scenario C

ITEM	COST	QUANTITY	TOTAL
VMware vSphere Standard	\$995.00	1	\$995.00
VMware vCenter Server Standard	\$4,995.00	1	\$4,995.00
Windows Server 2012 R2 Standard	\$882.00	1	\$882.00
			\$6,872.00

Table 4: Scenario C Budget

Actual

ITEM	COST	QUANTITY	TOTAL
VMware vSphere Standard	\$0.00	1	\$0.00
VMware vCenter Server Standard	\$0.00	1	\$0.00
Windows Server 2012 R2 Standard	\$0.00	1	\$0.00
Amazon Web Services Trial	\$0.00	1	\$0.00
Vmware Workstation 12 Pro	\$0.00	1	\$0.00
			\$0.00

Table 5: Project Budget

CONCLUSION

Small and medium sized businesses struggle with disaster recovery. They struggle in a variety of ways and for a variety of reasons. This project addresses the problem by providing resources to help SMB's with disaster recovery. Important planning concepts including RTO, RPO, and MTD have been explained. Strategies and concepts for DR solutions have been outlined. Finally, technical demonstrations in this project help stakeholders visualize and understand potential DR solutions. This project helps businesses by focusing on common constraints and simplifying disaster recovery.

NOTES

1. Symantec 2011 SMB Disaster Preparedness Survey Global Results January 2011
https://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey
2. "DOWNTIME, OUTAGES AND FAILURES - UNDERSTANDING THEIR TRUE COSTS,"
Winds of Change Blog, Evolven, September 18, 2012, accessed November 2015,
<http://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html>
3. "Creating and testing effective disaster recovery plans." *Database and Network Journal* Dec. 2007: 12+. Expanded Academic ASAP. Web. 15 Nov. 2015.
4. Symantec 2011 SMB Disaster Preparedness Survey Global Results January 2011
https://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey

BIBLIOGRAPHY

Symantec 2011 SMB Disaster Preparedness Survey Global Results January 2011

https://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey

“DOWNTIME, OUTAGES AND FAILURES - UNDERSTANDING THEIR TRUE COSTS,” *Winds of Change Blog*, Evolgen, September 18, 2012, accessed November 2015, <http://www.evolgen.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html>

Donna R. Childs, *Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Businesses* (John Wiley & Sons, 2008), page#.

“COSTS AND SCOPE OF UNPLANNED OUTAGES,” *Winds of Change Blog*, Evolgen, November 18, access November 13, 2015, <http://www.evolgen.com/blog/costs-and-scope-of-unplanned-outages.html>.

"Creating and testing effective disaster recovery plans." *Database and Network Journal* Dec. 2007: 12+. Expanded Academic ASAP. Web. 15 Nov. 2015.

Robert Bready, “Downtime and Data Loss: How much can you afford?,” *Analyst Insight* (August 2013): 1-5, accessed November 20, 2015, <http://www.aberdeen.com/research/8623/ai-downtime-disaster-recovery/content.aspx>.

“Quorum Disaster Recovery Report,” QuorumLabs Inc. (Q1 2013): 1-7, accessed November 20, 2015, <http://oneclick.quorum.net/rs/position2quorum/images/Disaster-recovery-report-Q1-2013-1031.pdf?aliId=13>.

Joshua Feierman, “High Availability and Disaster Recovery for Small Businesses,” *Simple Talk* (December 2014), accessed December 3, 2015, <https://www.simple-talk.com/sql/backup-and-recovery/high-availability-and-disaster-recovery-for-small-businesses/>.

"What Will You Use It For?" BackBlaze B2 Cloud Storage (n.d.) accessed March 20, 2016, https://www.backblaze.com/b2/b2-use-cases.html#disaster_recovery.

"Lowest Cost Cloud Storage Pricing," Cheapest Secure Cloud Storage Provider: B2, BackBlaze, accessed March 21, 2016, <https://www.backblaze.com/b2/cloud-storage-pricing.html>.

"EC2 Instance Pricing – Amazon Web Services (AWS)," Amazon Web Services, Inc. (2016), accessed March 21, 2016, <https://aws.amazon.com/ec2/pricing/>.

"Cloud Storage Pricing – Amazon Simple Storage Service (S3) – AWS," Amazon Web Services, Inc. (2016), accessed March 21, 2016, <https://aws.amazon.com/s3/pricing/>.

"VSphere and VSphere with Operations Management," VSphere Pricing & Licensing, VMware, (2016), accessed March 21, 2016, <https://www.vmware.com/products/vsphere/pricing.html>.

"How to Buy Windows Server 2012 R2," Windows Server 2012 R2, Microsoft (2016), accessed March 21, 2016, <https://www.microsoft.com/en-us/server-cloud/products/windows-server-2012-r2/Purchasing.aspx>.