

Our Colorado region is offering a FREE Disaster Recovery Review promotional through June 30, 2009!

This review is designed to help the small business better understand the state of their disaster recovery program. It will assess key elements of IT backup and recovery strategies, while introducing Advanced Integrators to companies in the Colorado market. Small business IT systems are a vital part of the organization and downtime or loss of data could negatively impact the business. Threats include hardware failure, fire, natural disasters, viruses, and a number of other events that could require the use of a disaster recovery plan.

With the latest features found in Microsoft products today adequately planning for disasters is more affordable than ever. Taking advantage of this FREE review will provide your company with a valuable report that can help you better prepare for a disaster and possibly show you inexpensive ways to improve your ability to recover from a disaster. A few pages of a sample report have been included below for your review.

To schedule your FREE review contact us at (303) 642-0290 or email us at Coloradoinfo@advancedintegrators.com and put FREE Promo in the subject line. We can schedule your FREE Disaster Recovery review and help you be prepared! Some limitations and restrictions apply to this offer.

Disaster Recovery Review

Small Business Technology Review

May 11, 2009

Client

Sample Company
Contact
123 Ridge Rd.
Golden, CO 80401

Consultant

Advanced Integrators, Inc.
Brian Stephens
PO Box 7361
Golden, CO 80403

Introduction

Disaster Recovery planning is frequently not fully implemented for many small businesses. This important function is often overlooked due to limited resources. The first step for any business to improve their Disaster Recovery (DR) plan is to identify possible disaster scenarios and evaluate the current state of the businesses DR plan. This promotional free DR review by Advanced Integrators will provide one of these first steps of the process, by evaluating your current DR plan.

With all the potential threats to your company data and information systems it is important to think ahead regarding mitigating downtime and loss of data. These threats can include: computer hardware failure, fire, natural disasters, human error, file corruption, viruses, and several other events that could impact your capability to conduct business activities.

This review is designed for small business IT environments with an assessment of the basic critical functions found in most small businesses. The topics covered are outlined below and the report will provide valuable information on the capability of the business to handle a disaster.

- I. Management Involvement
- II. Server Systems
- III. Desktop Systems
- IV. Application Software
- V. Communication Equipment
- VI. Vendor Considerations
- VII. Recommendations
- VIII. Summary

I. Management Involvement

Management Involvement is the first step in creating and maintaining a Disaster Recovery program. Management must evaluate possible disaster scenarios that could negatively impact business activity. The key elements of disaster recovery planning that management should consider are reviewed in the following tables.

Objective

Comments/Findings

Objective 1: Determine the involvement of management in the Disaster Recovery (DR) plan oversight and support.

<p>1. Determine if a planning group or process has been assigned the task of implementing and maintaining a DR program. Overall, this planning process should encompass the organization's DR strategy, which is the ability to recover, resume, and maintain all critical business functions.</p>		<p>Management has not formally documented a DR plan. It has put some measures in place to mitigate down time.</p>
<p>2. Determine whether the owners have ensured that integral groups are involved in the business continuity process (e.g. business line management, risk management, IT, facilities management, and audit).</p>		<p>Only a few of the individuals that work on the computer systems are involved in the disaster recovery process.</p>
<p>3. Determine if ownership has implemented a risk assessment, DR plan and testing program. This plan should include the impact and probability of disruptions of information services, technology, personnel, facilities, and services including:</p> <ul style="list-style-type: none"> ▪ Natural events such as fires, floods, severe weather, air contaminants, and hazardous spills. ▪ Technical events such as communication failure, power failure, equipment and software failure, and other disruptions. ▪ Malicious activity including fraud, theft or blackmail; sabotage; vandalism and terrorism. 		<p>A formal risk assessment and DR testing program has not been implemented.</p>

4. Determine if ownership oversees the timely revision of the DR and testing program based on problems noted during testing and changes in business operations.		With no formal DR plan, this process has not been completed.
---	--	--

II. Server Systems

The server systems used by small businesses can contain several types of critical data. This may include accounting, customer information, email, and other data that is used by the organization every day. The loss of this critical data or even the unavailability of data could negatively impact a small business. With the numerous options available today for properly securing data, a company should have some form of program to protect their server data. The following assessment of the server data backup and recovery programs will help address the consequences of a hardware failure, natural disaster, fire, human error, file corruption or other previously mentioned disaster.

The following servers were reviewed

Description	Comments
HP ML350 with HDW RAID 5	Server 2003 DC w/Exchange server, file & print services
HP ML310 with HDW RAID 1	Server 2003 Member server running Dynamics CRM

Objective _____ Comments/Findings

Objective 3: Determine the extent of server backup and recovery systems.

<p>1. Determine whether satisfactory consideration has been given to backup systems:</p> <ul style="list-style-type: none"> ▪ Has a backup application been set up with scheduled jobs. ▪ Does backup include nightly. ▪ Does backup include off-site ▪ What media types are being utilized for backup files. 		<p>A commercially available or Windows Backup system has not been configured for either server. A manual process of frequently coping files is being done by internal staff. The media for these copies is an external USB connected hard drive.</p>
<p>2. Determine whether satisfactory consideration has been given to hardware & software systems:</p> <ul style="list-style-type: none"> ▪ UPS on key server equipment. 		<p>The DC server is on a UPS sufficient to sustain power for a short outage. The member server is not on a UPS.</p> <p>Hardware RAID technology is used for both</p>

<ul style="list-style-type: none"> ▪ Is RAID technology utilized. ▪ Has redundant hardware components been considered. ▪ Has manufacture support contact information been documented. ▪ Is installation CD readily available. ▪ Has Recovery Console or Automated System Recovery been considered. ▪ Has the Startup and recovery options been configured. 		<p>servers helping to reduce downtime.</p> <p>The DC has redundant power supplies and the member server does not have redundant components.</p> <p>The install CD is readily available in the server room.</p> <p>The Recovery Console has not been installed for startup and ASR is not getting backed up. These Startup and recovery options have not been configured. Additionally the system state is not getting backed up.</p>
<p>3. Determine whether satisfactory consideration has been given to email & database backup systems:</p> <ul style="list-style-type: none"> ▪ Has a backup application been set up for email. ▪ Has a backup application been set up for database systems. 		<p>The email system is not getting backed up. The SQL database on the CRM system is not getting backed up.</p>

VII. Recommendations

Management Involvement

The organization has not documented or planned for a disaster. In an organization of this size this practice is not uncommon, but should a disaster occur some pre-planning would be beneficial. Since the organization does not have a complex IT environment it will not take much time to document some basic plans for disaster recovery. We recommend putting together a basic plan by identifying possible threats, implementing desired procedures to mitigate those threats, and reviewing the plan annually as business changes can require modifications to the original plan.

Server Systems

The server environment does not have sufficient back up procedures in place. This puts critical data and applications in jeopardy and could result in a downtime or loss of data that could negatively impact the business. The decision to purchase servers with hardware RAID technology and redundant components will help mitigate possible down time from failed hardware components. However, provisions have not been made for major failures that would require a server rebuild.

Our recommendation would include implementing formal backup procedures for both servers. There are a number of commercially available backup software applications which would meet your requirements, but we would recommend at the minimum to utilize the Windows Backup utility provided by your operating system. This simple backup software application can back up your system files, data files, application files and the system state files which are helpful for restoring a server. We recommend you configure the Automatic Recovery Service (ASR) feature, set up the Recovery Console tool, obtain System State Backups on a regular schedule and utilize the Volume Shadow Copy feature of the Backup Utility software tool to backup the Exchange Server application and Dynamics CRM application. These tools do not require you to purchase any additional software and numerous affordable media options are available to work with the software. A backup plan with provisions for some type of off-site storage would be ideal and there are a number of options for implementing such a plan. It could be as simple as having a trusted employ taking a copy of the backup files off-site to enrolling in a service that will remotely copy the backup files over the Internet. We also recommend you purchase a UPS for the member server and configure both server UPS systems with shutdown software.

These changes to your server environment will not require a significant expense, but should improve your recovery options significantly. Implementing these backup procedures and incorporating documentation and testing will significantly reduce potential downtime and expense should you have a disaster.