Newsletter

Celebrating 29 years serving Central, N.C.! *February 2019*

Disaster Recovery: Is Your Business Prepared?

When the term disaster recovery comes to mind most people think about these natural disasters -- tornados, hurricanes, blizzards, and more. However, in the small business world these types of disasters make-up only 10-14% of all disasters that severely affect businesses. The real question is: what makes up the other 86-90% of these disasters and how can I protect my company's data?

You may have guessed it: the most common issues are human error, security breaches, and the unfortunate equipment failure are some of the top reasons companies suffer. It is easy to think none of these problems will happen to you, but I assure you without a plan of action you are only hurting yourself. Len Oppenheimer's near disaster story should become a reminder for all of us.

Len Oppenheimer, Chief Executive of the Golden Box, a company that supplies packing materials for its clients in the tristate area in NYC was almost out of luck when a power surge in his office damaged an essential server. He said, "We had started doing backups literally three days before the server went down".

The Chief Executive went on to say,"If we hadn't had that safety net in place, I hate to even think about where we'd be right now." Before all of this scares you too much, there is good news: disaster preparation is always available. Knowing exactly how to prepare is crucial. Most companies that have experienced a disaster would consider constructing a recovery plan to be the best way to solidify your company's success while everything is collapsing.

Where to Begin:

First-things-first, define your need. Jennifer Walzer, an experienced small business owner and New York Times writer, asks the most important question,"If you walked into your office tomorrow and your data was gone, what would you miss the most?"

It may take some time to defined, but once defined you can create an action plan to make sure your data is recoverable. Sometimes this question is difficult to answer, and that is where an IT expert comes in. An expert can inform you on the best data backup support systems and design an infrastructure to fit your needs.

Perform an Audit:

Secondly, a recovery plan requires your company to perform an audit to determine answers to some of your business' life-or-death questions.

Continued on inside

Upcoming Events

Using LinkedIn as a Business Tool presented by Teddy Burriss
February 21, 2019

Legal Compliance Lunch & Learn presented by TCDI
March 7, 2019

Cyber Security Panel Discussion
April 11, 2019

For more information on our upcoming events, please visit https://www.tcsusa.com/calendar/.

Continued...

You should know how at risk your company will be if a disaster strikes and how much downtime is possible before matters become worse.

For example, you may have an employee that tends to cook soup or another lunch item on your company stove. Just this once she or he decides to leave the stove unattended to go to the bathroom. Only a minute or two later the food boils over and causes smoke to envelop the kitchen. Suddenly, the fire sprinklers rain down onto your in-house servers and company computers. Now, what?

If such a disaster strikes, it is necessary to create a fallback plan to keep your business running as smoothly as possible. A fallback plan should consist of a secondary location to do work or an alternative way to communicate with clients.

Disseminate the Information:

Next, before the plan is completely outlined with details and priorities it is best to give each employee a part of the recovery process, this distinguishes between what is supposed to be done and who is supposed to do it.

Owners and managers should disseminate this information to staff so they are in the know about recovery procedures. You may think it lacks importance, but communication is one of an essential aspects of the recovery process. For instance, if one of your employees clicks on a malicious link, instantly knowing their computer is infected with a virus you would rather them come to management instead of briefly glossing over the subject to another employee.

Practice, Practice, Practice:

However, none of this will work unless your company practices their plan alongside other mandatory mock natural disaster tests. Make sure your company is well-rehearsed, so employees can be held accountable for a real disaster.

Mock tests also include checking on backup systems frequently. All backup prevention support varies; therefore, your company should know how all your backup systems work.

As the years go on preparing for business continuity is becoming more imperative, especially for small businesses where a trivial disaster can knock them down with a single wave. However, disaster recovery plans can feel tedious and possibly a costly measure for something that may or may not happen. But, Len Oppenheimer can be our cautionary tale, by reminding us that unexpected things do happen. If you want to acquire further assistance or have additional questions about backups, Total Computer Solutions offers a no obligation review of your current solution.

The Major Causes and Solutions for Downtime

Downtime is inescapable. However, the top reasons for downtime are mostly IT-related. With issues ranging from Social Engineering to hardware failure, it is nearly impossible for companies to pay equal attention to every cause of downtime.

Fortunately, there are ways to limit the overall amount of downtime your company could endure. Here are the major causes and solutions for downtime:

1) Social Engineering

If a person uses deceptive methods to pressure you into sending personal information for their gain, then they are using Social Engineering against you. Hackers tend to use big-name organizations to scam a larger population. For example, Dropbox, the file sharing Internet Company, has had its own share of Social Engineering attacks. One bad actor lured its users to sign into a fake login page that was set up on Dropbox itself. Scams, such as these, could install malware, a virus, or Ransomware on your network, causing it to be down until your company's IT partner removes it.

2) Hardware Failure

Hardware failure is a major cause for network downtime because it is unpredictable. Worrying about deadlines and planning can quickly become unimportant if you experience a large-scale equipment failure. For example, an outdated server or generator outage, can cost money, not to mention loss of reputation and unhappy clients.

3) Software Failure

Another cause for downtime is software failure, which usually happens when a software provider does not test patches before clients receive them. Corruption of applications can occur from this, and eventually stop entire systems. Software failure can also happen when an operating system gradually dies, simultaneously causing the software to go too. Lastly, as always, viruses and malware can cause issues with software.

4) Natural Disasters

When we think of disasters, our minds usually go to the natural ones, including earthquakes, tornadoes, and hurricanes. Though Natural Disasters account for only four percent of downtime, they are still an issue for organizations, especially since they are the least preventable incident.

Continued on next page

Use these three ways to cut your network downtime:
1) Disaster Recovery Plan

When an incident occurs, your organization should have a step by step plan of action. Crises are never easy, but a rehearsed plan will make the incident more manageable and will hopefully take less time to find a solution to the problem. When a solution is in place, it can limit your downtime, essentially cutting profit loss.

2) Keeping Backups

Another important way to minimize the costs and consequences of downtime is to create backups. Keeping copies of data gives access to your work when the network is down. There are several ways to keep backups including the Cloud, Network Attached Storage (NAS), or Dedicated Backup Software.

Unfortunately, backups do not always work; therefore, one important thing to remember is to frequently test them. Not checking backups regularly could lead to data loss.

3) Installing a Disaster Recovery System

A Disaster Recovery System (DRS) is similar to a backup, but a DRS helps with major incidents. This system takes snapshots of a computer, saving everything from data to applications. Therefore, you will not have to worry about losing anything necessary for work, even if downtime strikes.

Need More Solutions for Downtime?

Network downtime is inevitable, but knowing the causes and the ways to cut downtime, can help an organization be prepared. For more information about network downtime, contact Total Computer Solutions at 336.804.8449.

Meet Our Team: Richie Adams

Please join us in welcoming Richie Adams to the TCS Team as our Technical Analyst. He has over six years of Systems Engineering and network experience. Richie graduated from West Virginia University Institute of Technology with a B.S. in Computer Science.

Microsoft Stops Supporting Windows 7

If you are still using Windows 7, now is an excellent time to consider an upgrade.

Starting January 14, 2020, less than one year away, Microsoft will no longer support Windows 7. After that you are on your own, your operating system will no longer receive technical assistance, updates or security patches.

Older PCs can be upgraded to Windows 10 if they are meeting the minimum requirements set by Microsoft. However, we recommend that users and businesses get a new computer instead of upgrading their older machines.

Often small and medium size business owners focus on short term costs, using the end of life software and hardware can end up costing you more money than it is worth.

When you are unable to complete transactions for clients, or your computer that continually stops or stalls during presentations and video conferences eventually will hurt your reputation. A computer that loses data can cost you a fortune.

If you would like more information or help to assess the age of your workstations, call today for a no-obligation consultation at 336-804-8449, and one of our consultants will contact you to discuss the best solution for your company.

Digital Newsletter

If you would like to receive our newsletter digitally, please visit tinyurl.com/ycqvv2r6.

Follow us on social media!

totalcomputersolutions

168 Thatcher Road
Greensboro, NC 27409

In this Issue:

webinar

Using LinkedIn as a Business Tool

Join us for our upcoming webinar!

Date: Thursday, February 21, 2019
Time: 11:00 a.m. ET
Cost: Free
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449.
Presenter: Teddy Burriss, Burriss Consulting

Learning Objectives

- Discover the best practices of building a professional LinkedIn profile.
- Understand the best practices and tactics of growing a relevant LinkedIn Network.
- Explore and learn the best practices of bulding a professioanl reputation using LinkedIn.
- Become aware of the value of using philosophies of Search Engine Optimization best practices of their LinkedIn Profile.
- Become exposed to the best practices of sending and receiving LinkedIn invitations focused on your business goals.
- Review the purpose and tactics of engaging with your LinkedIn in meaningful ways.