TCS

Newsletter

Celebrating 30 years serving Central, N.C.

February 2020

Disaster Recovery Plan: Is Your Company Prepared?

When the term disaster recovery comes to mind most people think about the slew of natural disasters--tornadoes, hurricanes, blizzards, and more. However, in the small business world these types of disasters make-up only 10-14% of all disasters. What makes up the other 86-90% of these disasters and how can you protect your company's data?

You may have guessed some of the top reasons companies suffer: human error, security breaches, and equipment failure. It is easy to think that none of these problems will happen, but without a plan of action you are creating the conditions for possible disaster.

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 NYC tristate area, 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 consider the construction of a recovery plan to be the best way to prevent total disaster.

Here are Four Steps You can Take

Step 1: Define your need

First thing 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 define, but once defined you can create an action plan based on this definition. An IT expert can inform you about the best data backup support systems and design an infrastructure to fit your needs.

Step 2: Perform and audit

Secondly, a recovery plan requires your company to perform an audit to determine answers to some of your business' life-or-death questions. You should know how at risk your company will be if a disaster strikes and how much downtime is possible before things worsen.

Upcoming Events

GMA After Work Network
February 18, 2020

Lunch & Learn: The Role of Backup in Ransomware Recovery
February 27, 2020

TCS Security Madness: Your Best Defense is a Good Offense
March 20, 2020

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

"Disaster Recovery," Continued

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.

Step 3: 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 is not important, but communication is one of the 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. Company culture is key, and company cultural practices with make a positive impact.

Step 4: 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 costly especially since the disaster may or may not happen. But Len Oppenheimer can be our cautionary tale, by reminding us that unexpected things do happen. We all know about Murphy's Law.

Follow us on social media!

NSA Discovers Deadly Security Bug in Windows 10

A recently discovered security bug in Windows 10 is so nasty that the National Security Agency reported its existence. If you have any Windows 10 machines, and have not updated since January 15th, 2019, run a system update now. The bug also affects Windows Server 2016 and 2019.

The bug is in Microsoft's CryptoAPI. It concerns cryptographic certificates, including X.509 certificates, which are the basis for HTTPS security. Malicious parties can use the vulnerability to spoof a website. A malicious public Wi-Fi hotspot could impersonate a trusted, supposedly secure banking or e-commerce site, and Windows would fail to detect the spoofing. It could read encrypted traffic in transit, stealing confidential form submission information.

The same bug lets a criminal modify an application for downloading and create a forged Authenticode digital signature, creating the impression that it is from a trusted source and has not been tampered with. Combining the two techniques would make it possible to impersonate a download site and deliver infected applications without being detected.

The Discovery of the Bug

This report represents a shift from the NSA's earlier practice of discovering security bugs and leaving them unreported so that it could use them for espionage. Their previous practice backfired when criminals stole its software to create the WannaCry ransomware. Anne Neuberger, head of the NSA's Cybersecurity Directorate, called its response to this issue a "change in approach" aimed at "building trust."

By reporting the present bug to Microsoft, the creation of a patch closed the vulnerability. It is inevitable, though, that many systems will not get the update for a long time, if ever.

The bug is formally known as CVE-2020-0601. The CERT notification provides technical details.

Windows 7 is reportedly unaffected by the problem, which is a good thing since support for it came to an end on the same day as the announcement. Even so, you should update any systems running Windows 8 or older to Windows 10 as quickly as possible. Any vulnerabilities in them that are discovered from now on will not get fixed.

Fixing the Problem

Military and selected private organizations got the patch under secrecy before the public announcement. It is now available to all licensed Windows 10 systems.

"Deadly Bug," Continued

If you have automatic updates enabled, you should already be in good shape. It does not hurt to verify that the updates are happening. If you do not use automatic updates, open the Start menu, and select "Windows Update." The January update fixes many other security issues at the same time.

As always, avoid panicked reactions. There will certainly be fraudulent email campaigns with "security fixes" that are malware. Use only standard update procedures through a trusted Internet connection.

If you have a lot of systems to update, give priority to endpoints that are connected directly to the Internet as well as Web and proxy servers.

Windows Defender and Microsoft Security Essentials have been updated to detect the threat, and they are available for older operating systems. They are not a substitute for an up-to-date system, but having multiple layers of protection is wise.

Keeping Up with Security Updates

Most security issues are not as alarming as this one, but weaknesses in applications and operating systems turn up regularly. It is essential to keep the OS and Internet-facing applications on your systems up to date with the latest security patches.

If your business does not have a dedicated IT staff, or if dealing with employee and customer issues takes up all your time, trusted professionals can assist in managing your system updates and security issues.

GMA AFTER WORK NETWORK

Date: Tuesday, February 18th
Time: 5:00 pm - 7:00 pm
Location: Total Computer Solutions,
5601 New Garden Village Dr., Greensboro

Bring your workday to a close at GMA's After Work Network. Come enjoy complimentary drinks and appetizers while you play the GMA networking sticker game. WIth over 150 attendees, this is the best way to meet new contacts in the Triad. Free to all employees of GMA member companies. Not a GMA member? You can still attend!

Meet Our Team: Matt McNees

Please join us in welcoming Matt McNees to the TCS team in Business Development. He is orginally from the Pittsburgh area and is a proud alumni of Penn State and UNC-G. Matt is a long time Greensboro resident where he lives with his wife and kids.

Windows 7 End of Life--We Have Reached the End

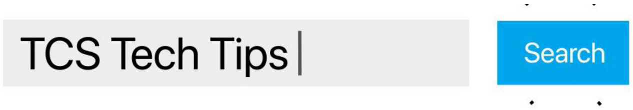
If you are still using Windows 7, now is an excellent time to upgrade because Microsoft no longer supports Windows 7. You are on your own as your operating system will no longer receive technical assistance, updates or security patches.

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 new computers instead of upgrading older machines.

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

When you are unable to complete transactions for clients, or you have a computer that continually stops or stalls during presentations and video conferences, your reputation could be affected. Plus, a computer that loses data can cost you an inordinate amount of business capital.

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.



Watch our new TCS Tech Tip videos! Visit tcsusa.com and click on our resources tab to find tips and tricks to help keep you more productive.

If you would like to receive our newsletter digitally, please email alimbers@tcsusa.com.

totalcomputersolutions

5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

totalcomputersolutions

The Role of Backup in Ransomware Recovery

Join us for our upcoming lunch & learn!

Date: Thursday, February 27th, 2020
Time: 11:00 am ET
Cost: Free
Presenter: James Moore, Client Strategy Manager, Total Computer Solutions
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449

Ransomware is running rampant, and your most valuable defensive tool is your backup. But the backup is more than just an extra copy of your files; it's an integral part of your ecosystem and, when properly configured, an asset and an advantage over your competition. According to the 2019 Global State of Channel Ransomware Report, the average incident costs $141,000, and the cost of downtime is now 23-times higher than the average ransom request of $5,900.

Let TCS show you how to tune your systems for maximum efficiency, and how to leverage your backup for maximum flexibility.

Key Takeaways:

- Why a "backup" is not just a software program, but an entire policy framework
- How to choose the best backup options to fit your expectations and budget
- Why you should invest in your backup solution like you do your primary systems
- How your backup helps you become more resilient against a ransomware attack