



Why a Disaster Recovery Plan is Valuable for Small Businesses

Some small businesses operate under the misconception that they are too small to be the target of cyber-attacks. The reality today though, is that cyber-criminals are most likely to target those businesses which they see to be most vulnerable. Cyber-attacks are much more likely to be directed toward the “low hanging fruit” of marginally secure small organizations as opposed to more elaborate attempts at breaching the data fortresses of large corporations with enormous security resources.

It is an accepted fact in the IT field today that the probability of cyber-attacks on any digitally active organization is not a question of “if” but “when.” 40% of businesses this year will experience network access by a hacker, and 50% will never even be aware that they have been hacked.

Cyber-attacks are just one form of disaster scenario beyond the control of enterprises. An effective BDR (Backup and Data Recovery) plan protects against data loss in any event, whether from natural disasters such as fire, flood, earthquake, or blizzard as well as data breaches caused by malicious actors

or simple human error. There are also the unpredictable risks of hardware failure and power outages, which are among the leading causes of downtime reported by businesses.

Data Loss Expenses and Business Failure Rates

According to the National Archives and Records Administration 90% of companies which experience just one week of data center downtime go out of business within 12 months. Companies lose an average of \$84,000 for every hour of downtime after a disaster. Even small data breaches of 100 files or less can cost a company between \$18,120 and \$35,730 according to a Verizon report at Entrepreneur.com.

An even more sobering statistic reported by the Gartner Group states that 43% of companies were put out of business immediately after a major data loss and another 51% went out of business within two years. That leaves us with a data loss survival rate of just a meager 6%.

The need for effective BDR plans encompasses all enterprises and organizations which rely on secure uncompromised digital data. While the disaster recovery needs naturally vary from business to business, there are elements of BDR which they all have in common.

Upcoming Events

GMA Noontime Network Online
July 17, 2020

Webinar: Backup & Disaster Recovery with StorageCraft
July 15, 2020

Webinar: Cyber Liability Insurance with Marsh & McLennan
August 11, 2020

Webinar: Your IT as a Business Journey
August 26, 2020

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

Elements of BDR

Data backup needs to operate consistently to ensure it is up to date and immediately available in the event of a server crash. The three components provide the ideal data backup include:

1. **Multiple incremental backups** throughout the day. Near real-time backups every 15 minutes.
2. **On-premise storage** of current data. A second copy stored locally enables quick recovery time, especially with large files which can be slow to pull from an off-site location.
3. **Off-site backup** is insurance against natural disaster losses. Off-site storage enables bare-metal restorations to get your new equipment online after the building has been unavailable because of disaster conditions. Off-site storage should be redundant in 2 locations, one locally for quick retrieval and one out of the region for natural disaster protection.

Scalable Pricing allows for vigorous business growth. As your business grows so will the data storage and application demands. A versatile BDR can grow with your business. Not all businesses require the most costly zero downtime BDR solutions, and more affordable BDR plans can be deployed based on, for example, a tolerable 2-hour downtime period.

Data Encryption ensures that data is not accessible to anyone on or off-site at the remote storage facility without a passkey.

Virtualization software can enable the BDR appliance to function as a standby server in cases where the physical server fails to restore on the device. The virtual image can provide a working server within 60 minutes of notification of the actual server crash while continuing backup of additional servers.

Bare Metal Restore is used to restore new or dissimilar hardware with the latest backup image.

Waiting for a server crash to test your organization's BDR plan can make any business a risky business. At Total Computer Solutions, we understand the need for businesses to mitigate the high risks of data loss while optimizing productive uptime. We can provide a thorough backup assessment to determine your organization's level of risk, and engineer, a total Backup and Disaster Recovery solution tailored specifically to the needs of your business.

Why Your Business is Not Prepared for a Disaster

Many business owners make a fundamental error when it comes to disaster recovery: they assume that their backups are working. Once those automated processes are set up, they merely assume that they are running smoothly, with few checks to ensure accuracy and capability. Then, the system goes down, or data is needed for recovery. That is when they discover that their backups are inadequate to their needs.

How Often Do You Back Up Your Data?

In general, we recommend that business owners back up their data every fifteen minutes. Unfortunately, some businesses still back up data only every thirty minutes or less--and some are still backing up manually at the end of the day. Consider the volume of data you go through every day: customer information, information about your products, and invoicing, to name a few. What happens if you lose that data? 93% of businesses who lost their data for just ten days had to file for bankruptcy within a year of the disaster--and half of them had to do it immediately. Can your business weather that kind of loss?

Are you checking Your Backups?

Many businesses have great backup systems in place. They might even be backing up every fifteen minutes, which means they will lose significantly less productivity if for some reason they need to rely on those backups. There is just one problem: they don't know whether or not those backups are running smoothly. Instead of evaluating their backups regularly, they are just assuming that they are working properly--and that can lead to disaster if you do have a data loss.

Are Your Backups Tough Enough to Withstand Challenges?

When you plan for backups for your disaster recovery, are you taking into consideration all of the challenges that could impact your business? Consider:

Your physical devices could be broken or stolen. In many cases, physical damage to your devices--including both tablets and laptops--can render them completely unusable. Consider the havoc that could result from an overturned cup of water on your desk or a thief who breaks into your car. If you lose your physical devices, do you have backups that will allow you to keep running your business?

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

Your business could be inaccessible. A disaster sweeps through your area, leaving your physical business inaccessible. Can you access your backups to get in touch with your clients and keep your business moving as smoothly as possible? If your physical building is destroyed by fire, flood, or another natural disaster, do you have the means to keep your business running anyway? Insurance can cover a lot of things, but it will not replace your data.

Your data could be deleted. All too many businesses have felt the horror of an accidentally-deleted piece of data. Worse, a disgruntled employee might decide to cause problems by deleting that data deliberately. Do you have a system in place that will help protect against those types of challenges, or are you relying on automatic backups that could also register that you deleted a specific file? How long do your backups go back? Could you restore a file deleted weeks or even months ago?

Ransomware can strike anywhere, any time. Ransomware could be devastating to your business as it locks your files away until you pay a substantial ransom--and sometimes, even the hacker who infected you will not provide the key. Sometimes, a bad actor will infect you more than once if you pose as a good target. When you have reliable backups in place, on the other hand, ransomware is a minor inconvenience from which you can quickly recover.

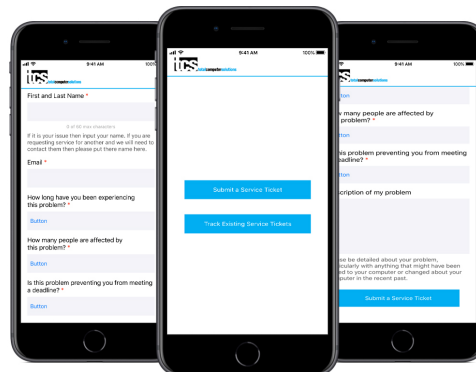
Regular data backups and a smooth-running network are critical to your business's overall functionality. Need more help with your overall security? Contact us today to learn how we can help.

Employee Spotlight: Darren Smith



Congratulations to our Client Strategy Manager, Darren Smith, for receiving his Cybersecurity Fundamentals for Sales and Cybersecurity Fundamentals for Engineers from ConnectWise. Cybersecurity Fundamentals teaches best practices for securing environments, best in class security tools, deep dive on incident response planning, intrusion detection, and malware analysis.

TCS App Available on the Apple App Store and the Android Market



TCS is thrilled to launch its new mobile app, now available for iOS and Android. We are continually looking for ways to improve our client's experience, and this new app provides users a new way to submit a ticket.

Two of our core values at TCS are effective communication, transparent exchange of information with mutual understanding and agreement, and continuous process improvement, getting better all the time. With these two core values in mind, we designed a tool for users that will improve communication.

We understand that our customers live busy lives and demand accessibility from a variety of different access points and devices, the app design keeps this in mind and ensures the screens are a useful experience across a range of devices.

The app's main objective is to provide current clients with an efficient and convenient way to communicate with us. Through the app, users can submit a service ticket and check on the status of existing tickets. The client portal will help streamline our ticketing process while providing the client with a service ticket catalog.

The easy-to-use modern interface makes it simpler for visitors to navigate rather than clicking through various layers of information online.

To install the app, please download directly from the App Store and Google Play. Your feedback will continue to help improve our customer experience and new features and design enhancements. To send any feedback regarding your experience on the new app, please email info@tcsusa.com.

If you are looking to add IT services to your business, contact us to discuss available solutions with an experienced and professional TCS team member.



5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

*Why a Disaster Recovery
Plan is Valuable for Small
Business*

*Why Your Business is Not
Prepared for a Disaster*

Employee Spotlight

*TCS App Available on the
Apple Store and the Android
Market*

GMA Noontime Network

Upcoming Events!



Date: Friday, July 17th

Time: 11:30 am - 1:00 pm

Location: Online

Miss your GMA friends? Want to find some new people to talk to? Like winning fabulous prizes? Bring your workday to a close with the GMA Noon Time Network you love...virtually!

Experience a NEW way to network online with GMA! While we may not have our famous stickers, we have a few tricks up our sleeve to help you break the ice and meet new contacts in a relaxed digital format akin to speed networking. Attendees will be placed in a series of small groups for networking that is both fast-paced and intimate.

Bring your lunch for this interactive networking event. Free to all employees of GMA member companies. *To register for the event, please visit www.tcsusa.com/events/.*