

## Did You Know?

### A DISASTER CAN PUT YOU OUT OF BUSINESS.

Everyone knows the importance of their data. What many don't realize is that while the chances of a major disaster are quite remote, the majority of data loss is the result of small localized problems. Could your business weather a major equipment failure caused by a hard drive crash, flood, lightning strike, or even theft?

**PCPlus Networks provides industry-leading solutions offering:**

- Business continuity and disaster recovery planning customized for your business needs
- Data backup and recovery to "bulletproof" your mission-critical data files

According to the US Bureau of Labor, 93% of companies that suffer a significant data loss are out of business within five years.

PCPlus Networks combines planning, prevention, and protection to make sure your business thrives no matter what comes your way. Let us protect your company against the disasters that can literally put you out of business. *Don't be a statistic.*

**Call us to schedule a free  
Disaster Recovery Analysis.  
PCPlus Networks  
678-523-5599**

**October 2021**



**This monthly  
publication  
provided  
courtesy of Shan  
Dholaria, CTO of  
PCPlus Networks**

"As a business owner, you don't have time to waste on technical and operational issues plus security is a BIG concern too. That's where we shine! Call us to put an end to your IT problems finally and forever."

# Protecting Your Business From Data Disasters

Data is everything to a small business in this day and age – which means if you lose access or control of your data, you lose everything.

As dramatic as that might sound, the data backs that up. According to several sources, 93% of companies, no matter how big they are, are *out of business within one year* if they suffer a major data disaster without having first formulated a strategy for combating it. And since 68% of businesses don't have any sort of plan for that worst-case scenario, that means losing data would be a death knell for most of the businesses in the country.

Fortunately, your business does not have to be one of them. By taking the following steps, you can ensure that you have a rock-solid disaster recovery plan in place.

### **Step 1: Know How A Disaster Recovery Plan Is Different From A Business Continuity Plan**

The main difference between these two types of plans is that while business continuity plans are proactive, disaster recovery plans are reactive.

More specifically, a business continuity plan is a strategy by which a business ensures that, no matter what disaster befalls it, it can continue to operate and provide products and services to its customers. A disaster recovery plan, on the flip side, is a strategy by which businesses can back up and recover critical data should it get lost or held for ransom.

So, now that we have a clear, concise understanding of what constitutes a disaster recovery plan, we can dive into the steps necessary to create one.

### **Step 2: Gather Information And Support**

In order to get the ball rolling on your disaster recovery plan, start with executive buy-in. This means that everyone, from the CEO to the entry-level employees, needs to be brought

*Continued on pg.2*

*Continued from pg.1*

in on executing the plan in case your company suffers a data disaster. When everyone is aware of the possibility of a data disaster, it allows for cross-functional collaboration in the creation process – a necessary step if you want to prevent breaches in all parts of your systems.

You need to account for all elements in your tech systems when you're putting together your disaster recovery plan, including your systems, applications and data. Be sure to account for any issues involving the physical security of your servers as well as physical access to your systems. You'll need a plan in case those are compromised.

In the end, you'll need to figure out which processes are absolutely necessary to keep up and running during a worst-case scenario when your capability is limited.

### Step 3: Actually Create Your Strategy

When everyone is on board with the disaster recovery plan and they understand their systems' vulnerabilities, as well as which systems need to stay up and running even in a worst-case scenario, it's time to actually put together the game plan. In order to do that, you'll need to have a good grip on your budget, resources, tools and partners.

**“93% of companies, no matter how big they are, are out of business within one year if they suffer a major data disaster without having first formulated a strategy for combating it.”**

If you're a small business, you might want to consider your budget and the timeline for the recovery process. These are good starting points for putting together your plan, and doing so will also give you an idea of what you can tell your customers to expect while you get your business back up to full operating capacity.

### Step 4: Test The Plan

Even if you complete the first two steps, you'll never know that you're prepared until you actually test out your disaster recovery plan. Running through all the steps with your employees helps them familiarize themselves with the steps they'll need to take in the event of a real emergency, and it will help you detect any areas of your plan that need improvement. By the time an actual data disaster befalls your business, your systems and employees will easily know how to spring into action.

So, to review, these are the quick actions that you and your employees will need to take in order to make a successful, robust disaster recovery plan:

- Get executive buy-in for the plan.
- Research and analyze the different systems in your business to understand how they could be impacted.
- Prioritize systems that are absolutely necessary to the functioning of your business.
- Test your disaster recovery plan to evaluate its effectiveness.

Complete these steps, and you can ensure that your business will survive any data disaster that comes your way.

## “I DIDN'T KNOW”

**Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.**

It's coming ...

- That day a hacker steals critical data, rendering your office useless ...
- That day when your bank account or credit card is compromised ...
- Or that day when your customers' private lives are uprooted ...

**Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself on how to PROTECT what's yours!**

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE “Cyber Security Tip of the Week.” We'll send these byte-sized quick-read tips to your e-mail in-box. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step

Get your FREE “Cyber Security Tip of the Week”  
at [www.pcplusnetworks.com/cybersecuritytips](http://www.pcplusnetworks.com/cybersecuritytips)



## Shiny New Gadget Of The Month:



### The LINK AKC Smart Collar

The world can be a dangerous place for a pooch who doesn't know any better; so, it's best to know how to keep tabs on your canine companion in case they bolt. That's where the LINK AKC smart collar comes in.

This smart collar is a comfortable and safe tracking alternative for your pooch. The LINK AKC smart collar comes equipped with several other useful features, including but not limited to:

- Activity monitoring and sound training specific to your dog's breed
- Temperature alerts if your dog is too hot or cold
- A place to digitally store vet records
- Waterproof features for up to 30 minutes in three feet of water

If you want your dog to be the greatest, highest-tech boy or girl out there, this collar is for you!

## Safe, Reliable And Unique ... Like A '63 Impala

For years now, I've told any business owner who will listen to "get different." If you've read my book of the same name, you'll know that it's not necessarily the better businesses that attract the most customers - it's the most different businesses. In an overly saturated market, the name of the game is standing out in the crowd.

Rather than just reshare the step-by-step guide that's in my book, I thought I would give a rather unique example of "get different" in action - and it's probably not anything you would expect.

Behold: Morris County's sheriff, James Gannon, and his '63 Chevy Impala. He might not be a businessman, but if he wants to garner votes for the next sheriff's election, he'll have to market himself nonetheless - and a classic police car is the perfect way to market what kind of candidate he is.

If you're having trouble picturing what a '63 Impala looks like, think about any classic police movie from around that era. The officer probably drove something similar, with the sleek body topped with a bulbous police light. If you saw that car driving up the street, what would you think about it? My guess is classy, old-school, bold, reliable, safe and just plain interesting. To his community, James Gannon is all of those things, if only by association with his Impala.

However, I should mention that Sheriff Gannon's car isn't some sort of misdirect; it's an accurate representation of who he is. Regardless of where you might fall on the political spectrum, you can't argue with his experience: 40 years in law enforcement and the security industry, working not only for his local police department, but also for the FBI, the prosecutor's office and finally as the sheriff in Morris County.

Sheriff Gannon's Impala accurately represents the fact that he is classy, reliable, bold, relatable and,



perhaps most importantly, safe. In a word, he's *different* from the other candidates. So, if you're looking to get different like Sheriff Gannon, let me finish up this article by giving you a few tips.

#### Find Your "Est"

Buying a car and outfitting it with your logo might not be the best move for marketing your business, but it should make you ask yourself these questions: What is your "est"? Are you the smartest? The fastest? The boldest? The most analytical, reliable or progressive? Find your "est" - what makes you unique - and run with it.

#### Stay Visible

Keep putting your business out there, even as you start to win business. Staying in the public eye is how you communicate to your market that you're confident in what you're offering, and that you're in it for the long haul. You want people to know that you're like Sheriff Gannon and his Impala - reliable and trustworthy.

The world is changing in so many ways right now. With your very own innovative marketing strategies, let everyone know that, through it all, your business vows to remain reliable and authentic. ~ Mike Michalowicz

### IT Security Tip: The #1 threat to your security is...

YOU! And your employees. Like it or not, human beings are our own worst enemies online, inviting hackers, viruses, data breaches, data loss, etc., through the seemingly innocent actions taken every day online. In most cases, this is done without malicious intent - but if you as a manager or owner aren't monitoring what websites your employees are visiting, what files they're sending and receiving, and even what they're posting in company e-mail, you could be opening yourself up to a world of hurt.

That's because employees' actions can subject the company they work for to monetary loss, civil lawsuits, data theft and even criminal charges if they involve disclosure of confidential company information, transmission of pornography or exposure to malicious code.

One thing you can (and should) do is configure your firewall to document and monitor which websites users are visiting. Almost all enterprise-level firewalls have this ability built in; you simply need to configure it and monitor the reports (something we can certainly help you with). But it's up to you to set the rules, write it into an Acceptable Use Policy (AUP), TRAIN employees on what is and isn't acceptable and then get them to sign the AUP.



1010 Lakes Pkwy  
Lawrenceville, GA 30043

### **Inside This Issue:**

- Protecting Your Business From Data Disasters
- Safe, Reliable, And Unique...Like A '63 Impala

## **3 Digital Disruptions That Affect WFH Employees And How To Avoid Them**

As more employees work from home, the risk of cyber-attacks grows. In 2020, between the months of March and July, nearly half of all businesses dealt with some sort of digital disruption. Some of the most common digital disruptions were:

### **Worker Productivity Losses**

When hackers infiltrate company computers, they might steal employee identities. This won't hurt your business directly, but it will indirectly, as workers have less time for work while they grapple with their identity being stolen.

### **Internet Of Things Infiltrations**

Now that so many "smart" devices can be hooked up to a central server, there are more avenues than ever for hackers to gain access to sensitive company data.

### **Ransomware Attacks**

Businesses of all sizes are falling victim to ransomware attacks, but it's the small and mid-size ones on a tight budget that really suffer from the fallout.

To stop these kinds of attacks, educate your workforce on best practices for avoiding hackers and make sure their systems are up-to-date with good cyber security software. Nothing is bulletproof, but you can do a lot to protect your company.