two river™
TECHNOLOGY TIMES

What's New

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.

October 2021

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and 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

Continued on pg.2

Continued from pg.1

brought 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.

"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."

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.

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 ahead of the bad guys. And because so few people know about these security secrets, every week you'll learn something new!

To request more information, email kmarquez@tworivertech.com

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 goodest, 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 is a very successful author, entrepreneur and lecturer. He has written several successful books, including his latest, Get Different. *He is currently the host of the "Business Rescue" segment on MSNBC's* Your Business, *and he previously worked as a small-business columnist for* The Wall Street Journal.

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

TRTG Happenings

DID YOU KNOW?

A recent security survey showed that…

45% of respondents did not change their passwords in the past year, even after a data breach occurred.

83% would not know whether their information was on the dark web.

92% of users are creating passwords that may contain public information.

A complex password is a necessity in the current age of cyberthreats, data breaches and other security incidents. Those of us who live in reality also know how hard it is to keep the seemingly hundreds of passwords straight, secure and different. Wait, what's that? All of your passwords aren't different?

Why is having different passwords so important? When an online retailer, or a website, gets hacked, oftentimes all you hear in the news is about how many credit cards were lost or what the financial damage was. You rarely hear about the user accounts that were compromised. However, if you have an account on a compromised website, the username and password you used very possibly could be published and available to anybody who wants to look at it at on the Internet. A clever crook knows that you probably use the same password on the compromised website as you do on your eBay, Amazon or other online account that may have a bank account tied to it. A good enough chance that they're likely to try it anyway. Sure enough, when you used the same password on your eBay account that you also used to set up an account on the compromised website to reserve hotel rooms, buy clothes or whatever else, the hacker now has your eBay credentials.

It is possible to keep the password madness under control. Ask us for tricks to having unique but memorable passwords. You might be surprised by how easy it really is. The bottom line is that no matter how much of a pain it is, it is very important to have different passwords for each online account.

Beware of this new/old scam

We're seeing a new variant of an old scam. Here's what happens: an employee gets an e-mail from their boss – who is traveling – to please send him, as soon as possible, scanned copies of all the W2s the company issued at the end of January. The message appears to come from their manager, including having what looks like the manager's actual e-mail address in Outlook. The employee gets suspicious – they has just talked to their boss on the phone that morning, and it was never mentioned that this information was needed. Before the employee collects the W2 PDFs that are on the HR drive, they decides to text their boss and check on it. Great catch! The boss never requested that information. Had the employee not been proactive and instead just completed the task assigned to them, they would have provided a scammer with all of the confidential information that is on a federal W2 form for every employee in the company! The scammer likely would have used the information to commit identity theft and/or file false returns next year to claim the refund.

Always be vigilant and proactive – it's better to be suspicious and double-check everything when dealing with confidential information. Try to provide that detail in an encrypted e-mail, or at minimum with a password on the files (and don't include the password in the body of the e-mail!). The few extra minutes it takes could save months of heartache for all of your employees.

Routers are $100 at the big-box stores-why do I need a $900 firewall AND pay a maintenance fee?

Routers and firewalls can be confusing – they essentially serve the same purpose of distributing Internet to devices on the network. A router like you'd purchase at a big-box store is designed to serve the needs of home, not the needs of business. It's likely more important that the Xbox has a great WiFi signal so little Jimmy can play his game, rather than being able to deny all Internet access from North Korea. A firewall, unlike a router, is intelligent. You typically pay a subscription fee because the firewall is constantly updating itself to protect against the newest cyber-attacks. Unlike a router, the firewall actually looks at all Internet traffic passing through it to make sure it's legitimate, not a virus, and was requested from a computer inside. They also allow us to block access totally to some third-world countries known for producing cyber-attacks. A good firewall can also let you know what your staff has been up to – who's that looking on careerbuilder.com for five hours? Don't cheap out, and don't buy your gate to the Internet for your business at a big-box store. It truly is the gate between your business and the rest of the world – and you want a strongly armed guard, not a non-intelligent robot. If you can afford to invest in one thing, get a good firewall!

PS – Business-grade firewalls can be used in homes, too – especially if you want to control the content users can access on the Internet, and want to see what the people in the house have been doing. There is no rule that a firewall is just for business – we sell them for use in the homes of lots of CEOs, CIOs and other professionals.