TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

June 2018

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Company Lessons from Hurricane Harvey

As another hurricane season approaches, here are a few lessons learned from Houston that can help.

Last August when Houston got slammed by Hurricane Harvey, now known as the most significant tropical storm in United States history, some companies were able to avoid the worst of the damage that Harvey handed out. That's not to say that they made it through the wettest week in Houston's history— over 60 inches of rain— unscathed. While some mitigated much of the damage through organization via the cloud, planned emergency communication and contacts who were put on high alert, even years of experience dealing

with floods and hurricanes couldn't keep them totally in control.

Corporate offices were completely flooded, but many well-prepared companies expected the flooding and had already moved vulnerable and important equipment and documents to higher ground. These were small and simple measures to take, but with another hurricane season fast approaching, it's important to nail down what your plan will be to keep your company operating as smoothly as possible.

Once a storm hits, communication can be tough. Staff and contract workers are stuck at home, electrical service can be spotty and without a dependable way for everyone to communicate, it's difficult to stay organized and know what needs to be done.

These days, smartphones and texting are a solid first line of communication to lean on, but during Hurricane Ike, not everyone knew how to send a text message, and cellular service was spotty. Fortunately, companies now have clouds to fall back on.

One property management company at the time had a Citrix ShareFile spreadsheet already created and shared with key staff. They were able to make real-time updates about property damage, important contact numbers, and notes about resident, unit, or management status. They were able to efficiently communicate among themselves and to clients during a major disaster because of their smart planning and due diligence. Without cloud-based access to a master document to organize their efforts, no one would have been on the same page at the most crucial moment.

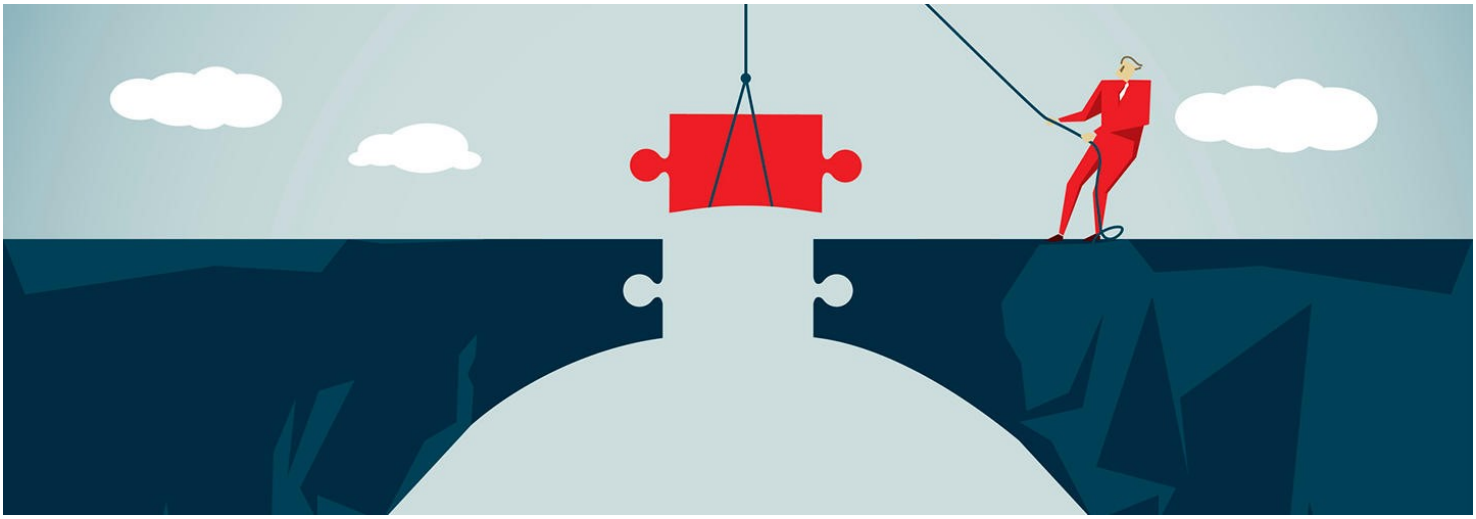
The worst thing you can do for your company in the face of a hurricane is to procrastinate before taking precautions. Before a hurricane reaches land, it's critical to take time to get things done while you still can. Have staff contact the employees at each of your locations to fill them in on what to expect regarding the weather and potential damage at that location. A team should visit each of your business locations a couple of days before a weather event is forecasted to begin to prepare the first-floor for flooding. Headquarters IT assets and property IT assets need to be as secured and elevated as possible.

You can live without most furniture, but not your essential business tools.

During a storm you'll find that lots of people you hoped to depend on are stranded without a car, working on other jobs, or otherwise unreachable. Priorities change in a heartbeat. That's why you'll need to have a go-to list of vendors and contacts that goes beyond the people you would typically call for specialized services and repairs.

As part of your disaster preparedness plan, always have more than one option when you're calling for repairs, and make sure you have a list of people you can call who are located in different parts of your region. Just one mile can make a difference in an emergency. It's important to start creating that network now, when it's not raining, so you'll have an extensive list to fall back on when unexpected weather occurs. Then, make sure you're on the phone with those vendors making plans in the days before a hurricane arrives. It can mean the difference between property being ruined by water damage and tackling problems head-on with proactive relationships.

Be sure to proactively plan out all of your resources: your people, data, tools, processes and vendors. It pays off in ways that you can only fully appreciate once you find yourself standing in feet of flood water.



How Your Small Business Can Create the Best Disaster Recovery Plan Possible

Are you and your business prepared if a disaster strikes? More disasters are happening now more than ever, fueled in part by climate change. Extreme weather events — most notably hurricanes Harvey, Irma, and Maria — caused a total of $306 billion in damage in the United States in 2017, making it the most expensive year on record for natural disasters in the United States, according to the National Oceanic and Atmospheric Administration.

Given this expected future, your small business needs to ensure that it has a robust and reliable disaster recovery plan in place. Why? Your business depends on it; **roughly 40 to 60 percent of small businesses never reopen their doors following a disaster**, according to the Federal Emergency Management Agency. Keep in mind that disasters include not just natural ones, but also system failures, security breaches and human errors that cause your business to go dark.

Before a disaster hits, your business needs to ensure its data is backed up and IT equipment is in place to return to business with minimal downtime. Replication of your data, cloud backups, and failover sites are just a few elements that make up a successful recovery plan. All of it requires detailed planning. Here are some of the key elements you need to create the best DR solution possible.

Disaster Recovery Starts with Assessments and Planning

The first step in creating any successful DR plan is to assess your small business's needs, requirements, budget and IT environment. IT leaders need to determine how disasters could affect the business and work with other company stakeholders to create a comprehensive DR strategy that encompasses people, processes and technology.

It comes down to examining each of those areas, and asking: 'How will we recover our technology? What processes need to be in place? And what are the redundancies at the people level?' You have to look at redundancy across the organization to figure out what the processes are for different threat scenarios.

That can be difficult for many small businesses to do, especially ones with a small IT staff. Thankfully, managed service providers can help conduct those assessments and work with you to set up DR plans.

You need to create a detailed business continuity plan that spells out how your business will respond to a disaster, ensure that it is widely known throughout the company, and update and test it regularly.

Redundancy is Critical to Any Disaster Recovery Plan

It's crucial that you back up your business's data, including customer data, in multiple locations. Businesses need to then replicate their files. During replication, files are copied from a primary location to a secondary location for use in the event of a disaster. Businesses should also consider virtualization and hyperconverged infrastructure to increase the redundancy of their IT environments, as well as backing up their data in the cloud.

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

Large cloud providers ensure availability of business-critical data by replicating it to a secondary data center region far away from the primary one. So, if an unforeseen event takes the primary location offline, you're still protected.

In addition to backing up data, small businesses should ensure that they can set up telework capabilities with mobile devices, cloud services, or virtual desktop environments. You should also consider subscribing to multiple internet service providers and other measures to ensure IT redundancy.

While all of this sounds like a lot, it's worth it. You don't want your business to lose revenue or fail because you did not adequately plan for a disaster. And a disaster may never come — but if it does, you should follow the Scouts' motto: be prepared.

What happens when legislation in one country affects what people do in other countries? The EU's General Data Protection Regulation (GDPR) took effect May 25, but what does that mean for you and me if you don't live in one of the EU countries? Cloud providers have been especially concerned about this since cloud services are intended to be available always, everywhere.

Alex Bordei, Director of Product and Development at Bigstep, answers some questions that may address some of your concerns.

Can you summarize in an easy-to-understand way what companies — whether they're users of the cloud or cloud providers — will face with the EU's GDPR requirements?

There are many levels of integration between companies and cloud services. But in all occasions, as some customer personal data might end up on a third-party's hard drives, that will be a form of "processing" and that will make the cloud provider a "processor" on behalf of the respective company. Storage alone is considered "processing" even if the data is encrypted.

Nowadays, most companies use cloud services, such as Google Analytics, Office 365, Salesforce, or AWS. All of them are external, third-party "processors" of data but do not necessarily handle end user's personal data. Under the GDPR, companies will need to be aware of these kinds of relationships and will need to track personal data as it flows between all these different vendors so that at any time they need to be ready to delete (right to be forgotten) or retrieve (data portability) all data pertaining to a particular customer (data subject).

Companies are now required to have a due diligence process in place to verify the cloud provider's security capabilities before sharing personal data with them. How this process looks is up to the company in question and depends on the actual data being processed. In case of a data breach, if the fault lies with the cloud provider, the company can be liable to those big fines if the due diligence process was not properly conducted when the contract with the cloud provider was signed. There is no "Compliant with GDPR" certification that cloud providers need to demonstrate but the provisions speak of a principle rather than a strict implementation requirement. Companies need to demonstrate a risk mitigation approach to data protection, meaning they need to actively think about what could happen to their customer's personal data and try to address those risks.

What obligations should people expect their cloud providers to meet?

There is no strict list of requirements. It's what satisfies the company doing the due diligence and relative to the data at hand. The risk here is to consider that the big cloud providers are safe just because they're big. The size of the cloud provider is not a security guarantee and does not absolve the company from doing due diligence. For instance, you have a system running in Microsoft Azure. The fact that it's Microsoft's brand name in there does not protect you from hackers that exploit your web-facing application's vulnerability nor does it provide you any guarantees that a rogue Microsoft employee might not find ways to go around your firewall.

The best thing is to think about possible risks (like the rogue employee stated above) and ask the cloud provider to provide details on how they mitigate that risk — and write the answers down. If satisfactory, then move on, if not, then look somewhere else. In the case of breach, you might be asked to demonstrate that you asked the questions and that the answers were OK. A word of caution on beta or alpha services: They are typically a lot less secure than their generally available (GA) counterparts.

As stated by the "privacy by design" principle, I would suggest you consider any cloud provider and your internal systems unsafe and try to not store plain text data in the first place. Actively encrypt, anonymize, pseudonymize, and generally build multiple layers of protection, not just a perimeter fence (a.k.a firewalls) around critical data.

From privacy by design to the transfer of data over international borders, what other obligations are cloud providers required to meet?

Companies should always be aware of where in the world the servers used to provide the service consumed are. If it's not immediately obvious, companies need to ask for clarification because GDPR states that personal data should not move across the EU boundaries without the customer's consent and implicitly the company is liable if that happens. Cloud providers are also liable under GDPR to fines if they move the data with the

controller's knowledge. The problem is the cloud provider might not be aware that there is personal data in a ZIP file, for instance, so it might be backed up on servers on the U.S. This is why you need to ask your cloud provider not only where the servers are but also if there are back up or synchronization processes happening that might touch that data.

Since all companies will ask the same questions, I expect cloud providers to provide comprehensive documentation on the above so chances are the answer to those questions is already readily available online.

Why do you think GDPR will ultimately help users as well as companies to advance into the next technological age and use of data?

I think there is a growing climate of mistrust in the Internet itself, amplified by Cambridge Analytica or the huge data breaches happening recently. This could lead to a kind of technical hypochondria that could prevent some portion of end users from using the Internet and online services to their full potential. As a society, it could set us back decades and billions could be lost in terms of opportunity cost. We might lose the elderly or other disadvantaged categories from increasingly using these services and this will in turn further segregate our society. These things don't happen overnight but doing nothing can cause widespread damage over time just like climate change.

GDPR is a step in the right direction because it forces managers to actually sit down and think about protecting the data of their users. Most companies out there truly want to protect their customer's data. In the end, we're all consumers of some company's services or another. We just did not stop and

2018's Cutting Edge Network Security Solution:

Cisco Umbrella

Cloud Delivered Enterprise Security

As the industry's first Secure Internet Gateway in the cloud, Cisco Umbrella provides the first line of defense against threats on the internet.

As a secure internet gateway, Cisco Umbrella helps you tackle the challenges of mobility, SaaS, and branch transformation by offering a single platform that secures access to and use of the cloud, SaaS applications, branch offices, and endpoints.

It's your first line of defense against threats -- anytime and anywhere your users access the internet, traffic goes through Umbrella first. By delivering security from the cloud, not only do you save money, but it also provides more effective security. Here's how:

1. DNS & IP layer enforcement

Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections. Stop malware before it reaches your endpoints or network.

2. Intelligent proxy

Instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection.

3. Command & control callback blocking

Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers. Stop data exfiltration and execution of ransomware encryption.

Call Tech Hero today to sign up for your free trial!

(800) 900-8324 x2

think about how to protect them behind a kind of corporate "cannot happen to me" thinking. I think companies already have so much control over people's lives, they need to become responsible for safeguarding them. They have an increasing responsibility not just to their shareholders but to society itself.

Client Spotlight

FLORIDA HOSPITAL

The skill to heal. The spirit to care.®

Our mission strengthens our commitment to health care. Because of our faith as part of the Seventh-day Adventist Church, we focus on healing the whole person–mind, body and spirit.

In fact, Seventh-day Adventists believe that spiritual and emotional health are vital elements to overall well being. It is this belief that guides us in all we do at Florida Hospital and it has helped us to create one of the finest health care facilities in the U.S., if not the world.

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.