PALMTECH
I.T. Solutions For Business
THE PALMTECH TIMES
PalmTech Computer Solutions June 2020

Are You Prepared For A Busy Hurricane Season?

Even if you feel your business is not likely to face the brunt of a hurricane's landfall, you should take steps to prepare for hurricane season. With talk of a busy hurricane season ahead, it is important that any business which might face heavy storms takes extra precautions. Extreme weather of any kind, from tropical depression and storms to Category 5 hurricanes and tornadoes, can not only cause structural damage to your business, but can also cause catastrophic data loss and network damages.

Visit www.palmtech.net/business-resilience/ to download our Storm Preparedness Checklist!

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Making This One Mistake With Your Network Can DESTROY Your Business

A lot of businesses wait until something breaks before they fix it. And even then, they may take a "patchwork" approach to fixing the problem. They are reactive rather than proactive. Sometimes taking a reactive approach is fine, but other times, and depending on the circumstances, it can lead to even bigger problems.

When it comes to network security, for example, being reactive to problems can be downright dangerous. It's not just hackers you have to worry about. There are power outages, data loss, equipment failure and more. In IT, a lot can go wrong. But if you're proactive about cyber security, you can avoid many of those pitfalls.

Reactive IT support used to be the norm. Most network security specialists went to work after something went wrong. Unfortunately, some businesses still have this reactive mindset when it comes to their IT and network security. They have an "it won't happen to me" attitude. The truth is that these are the people most at risk. It's not a matter of if, but when. Hackers and cybercriminals are more active than ever.

Thankfully, proactive support is now the norm. More and more IT services and security firms have the tools and resources to protect you BEFORE the worst happens. So, why partner with an IT services company?

There are many reasons why it's a good idea. One great reason that doesn't

continued on page 2

often get talked about is that working with an IT services company is an added value for your customers.

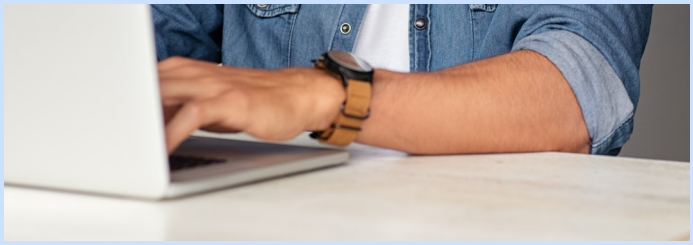
When they know you're taking IT security seriously – and when they know their data is safe – their trust in you is boosted.

When you build trust, you build loyalty, and customer loyalty is getting harder to come by these days. Plus, happy, loyal customers are much more likely to refer you to others who may be in need of your services. That alone makes investing in proactive IT security worth it.

Here's another reason why working with a proactive IT services firm makes sense: it's MUCH easier than trying to do it yourself. Many small businesses simply don't have the resources to hire an internal IT specialist or a team. Not only can that be very costly, but it's also rarely practical. Think of it this way: if you hire an IT specialist to handle your network security, manage cloud backups and provide general IT support, then what happens when they take a day off or take a vacation?

Having a dedicated IT specialist on your team isn't a bad thing, but they can be stretched thin very easily. You could be left with gaps in your support should anything go wrong. Suddenly, you don't have anyone you can call. Working with a dedicated IT services firm solves these problems.

> **"Unfortunately, some businesses still have this reactive mindset when it comes to their IT and network security."**

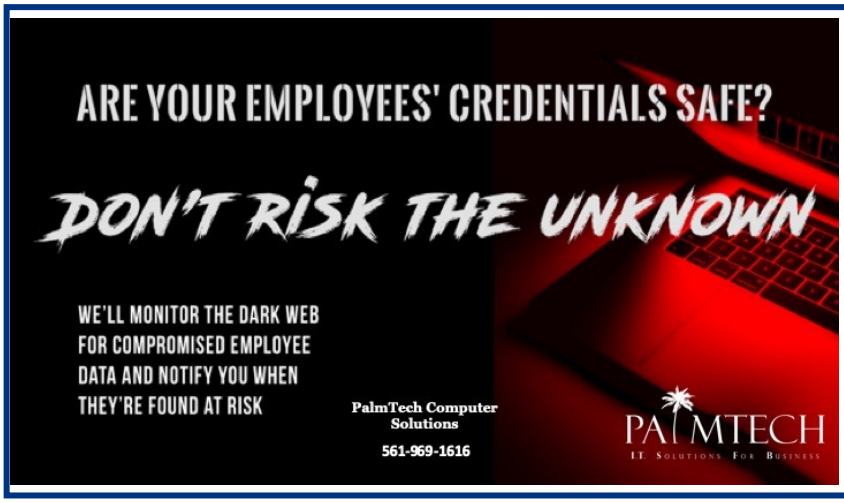


To take that a step further, good IT services companies are also great at catching problems before they become problems. They can catch things that might not have even been on your radar. For example, if your cloud backup service isn't backing up your data correctly or is backing up the wrong data, they'll catch that. Maybe you're saving data that's not properly encrypted. They'll catch that. Maybe you have an employee using software that's months out-of-date. Again, they'll catch that.

When you call up an IT services company and say you want to take a proactive approach to your network security, they should be willing and able to provide just that. An experienced firm will have a team with the training, certification and experience required to tackle today's cyberthreats while managing your network's day-to-day needs.

They know IT because they live IT. They help with data recovery should anything go wrong; they are your help desk when you have questions or concerns and they keep your on-site malware protection up-to-date. They are tailored to your business's specific needs. And as you grow, they adapt to your changing needs.

Put an end to the outdated way of thinking about IT security. It's time to be proactive and to recognize your company's vulnerabilities before they become vulnerabilities. You just have to make the call to us at 561-969-1616.



Are Your Employees' Credentials For Sale On The Dark Web?

Visit
www.palmtech.net/darkweb/
For A Free Scan!

The Many Faces Of Corporate Leaders

Employees' happiness at work is more important in the workforce than ever before, and that feeling of fulfillment and engagement often comes from the top. If you are aware of what type of leader you are and how your leadership affects employees and clients, you can mitigate your weaknesses and discover your strengths to ultimately lead more effectively. Let's take a look at a few leadership personas I've witnessed while coaching and what works best for each.

In-The-Weeds Leaders
Leaders who are "in the weeds" tend to spend too much time in the day-to-day. They get bogged down with what's in front of them and don't think outside the box. Without innovation, the company runs the risk of coming to a grinding halt.

These leaders need to delegate current tasks to their team members. They can then focus on finding new ways to drive the business forward. In-the-weeds leaders may even need an outside party to hold them accountable for setting and reaching these new goals.

Frustrated Leaders
These leaders know their companies can be better, but they're upset because they can't scale at the rate they want. They bottle up their grievances and aren't sure where the disconnect is with their teams.

These leaders could seek guidance from a third party, whether that's a friend or colleague. An outside perspective can help identify problem areas. They also need to hear out their team members and get firsthand accounts on what's not working. Both perspectives can help turn frustration into focus.

Mindful Leaders
These leaders recognize that rapid growth is positive as long as they scale appropriately with formal organization and efficient processes. They are careful to avoid pushing forward blindly and losing essential parts of their culture and values along the way. However, they may take too long to think things through and miss new opportunities that come along because they couldn't act quickly enough.

These leaders should make sure they are sticking to the systems they have in place while remaining open to new opportunities and evaluating them in a timely manner.

It's important to constantly reevaluate and adapt as the company grows and changes shape.

Control Freaks
These leaders can't seem to let go of the wheel. They micromanage and don't trust their team to get the job done, which fosters an atmosphere of frustration and mistrust. In this atmosphere, they can no longer lead effectively.

They should work with their teams to identify why the company exists, what motivates team members and why their work is important. That will not only help the leader and the team establish a better dynamic, but it will also help them both understand where the company is now and where it's going.

When evaluating your leadership style, be honest with yourself. If you can pinpoint where you are on the leadership spectrum, then you'll better account for your challenges and capitalize on your assets. And that's how you become more self-aware and, in turn, a much stronger leader.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

How Does the Dark Web Impact Businesses?

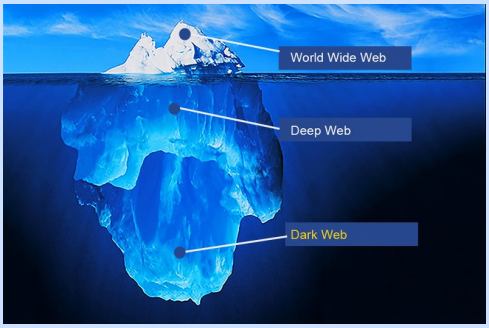
Identity theft is an unfortunate occurrence that is all too familiar with most business owners, but do those individuals know where the compromised data will end up? Often, these business owners are unaware of the virtual marketplace where stolen data is purchased and sold by cybercriminals; a place known as the "Dark Web".

What is the Dark Web? The Dark Web, which is not accessible through traditional search engines is often associated with a place used for illegal criminal activity. While cybercriminals tend to use the Dark Web as a place to buy and sell stolen information, there are also sites within it that do not engage in criminal activity. For many, the most appealing aspect of the Dark Web is its anonymity.

What is for sale on the Dark Web? Information sold on the Dark Web varies, and includes items such as stolen credit cards, stolen account information from financial institutions, forged real-estate documents, stolen credentials and compromised medical records. Even more alarming, the Dark Web contains subcategories allowing a criminal to search for a specific brand of credit card as well a specific location associated with that card. Not only can these criminals find individual stolen items on the Dark Web, but in some cases, entire "wallets" of compromised information are available for purchase, containing items such as a driver's license, social security number, birth certificate and credit card information.

What is stolen personal information used for? When stolen information is obtained by criminals, it can be used for countless activities like securing credit, mortgages, loans and tax refunds. It is also possible that a criminal could create a "synthetic identity" using stolen information and combining it with fictitious information, thus creating a new, difficult to discover identity.

Why are stolen credentials so valuable? Stolen user names and passwords are becoming increasing popular among cybercriminals, but why? Identity thieves will often hire "account checkers" who take stolen credentials and attempt to break into various accounts across the web using those user names and passwords. The idea here is that many individuals have poor password practices and are using the same user name and password across various accounts, including business account such as banking and eCommerce. If the "account checker" is successful, the identity thief suddenly has access to multiple accounts, in some cases allowing them the opportunity to open additional accounts across financial and business-horizons.



Why should businesses be concerned about the Dark Web? Since the Dark Web is a marketplace for stolen data, most personal information stolen from businesses will end up there, creating major cause for concern. With the media so often publicizing large- scale corporate data breaches, small businesses often think they are not a target for cybercriminals, however that is not the case. Cybercriminals are far less concerned about the size of a business than they are with how vulnerable their target is. Small businesses often lack resources to effectively mitigate the risks of a cyberattack, making them a prime target for identity theft as well as other cybercrime.

At a recent Federal Trade Commission (FTC) conference, privacy specialists noted that information available for purchase on the Dark Web was up to twenty times more likely to come from a company who suffered a data breach that was not reported to the media. The FTC also announced at the conference that the majority of breaches investigated by the U.S. Secret Service involved small businesses rather than large corporations.

How can you reduce the risk for your small business? To reduce the risks of a cybercriminal gaining access to your company's information/network, you must ensure you have proper security measures in place. The FTC has a webpage that can assist with security options for businesses of any size. In addition, it is crucial that your employees are properly trained on security, including appropriate password practices. There is also talk of a government-led cyberthreat sharing program which would help enhance security across all industries by sharing cyberthreat data.

Our senior security consultants would be happy to assess your business network to discuss your existing vulnerabilities and recommend how you can strengthen your security. In addition, we offer cyber awareness training for your staff so they can be your first line of defense. Call us at **561-969-1616** or email us at **info@palmtech.net.**