PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions October 2017

Businesses Survive Disasters With Virtualization

Hurricanes Harvey, Irma and Maria caused millions of dollars in damages. Some of that damage was unavoidable, but hundreds of businesses managed to stay open thanks to innovative virtualization solutions. If you're not already taking advantage of this technology, it's time to find out what you're missing.

Read More Here:
www.PalmTech.net/survive-disasters/

PALMTECH
I.T. Solutions For Business

October 2017

This monthly publication provided courtesy of Chuck Poole, President 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.

You're Better Off Giving Your Employees A $1,000 Bonus Than Being Cheap With Technology

Imagine, for a minute, that you're the CEO of a scrappy, promising new start-up. In the beginning, it was just you and two other employees working on dinky PCs out of a 12-by-12-foot office, but times are picking up and the company is heading into the uncharted waters of rapid growth.

As the business moves into the public eye — and, in turn, the hungry eyes of potential hackers — it's become obvious that you're going to need to lock down your data. At this critical stage, a cyber-attack could mean the death of everything you and your team have built.

But the budget is looking lean. Everything you've done so far has been by the skin of your teeth, so why should security be any different? You put one of your more tech-savvy employees on the case, tasking him with finding the cheapest cyber security solutions available. Sure, he may not be an expert, but he understands computers. What could go wrong?

He scours the web, perusing dozens of "Top 5 Cheap Firewall Software" articles, and, with the help of a scrappy how-to guide, installs what seems to be the best of the lot on your servers and across all your computers. The entire process takes 10 hours, and costs the company next to nothing.

Potential crisis averted, you turn your attention to other matters. We'll revisit our cyber security later, you think, once we have a little more financial wiggle room.

continued on page 2

Across the following year, the company's success skyrockets. The phone is ringing off the hook, new business is flooding in and your profit margin is exploding. You even ended up snagging a feature in Entrepreneur magazine. Your company is the envy of all your peers.

That is, until the day that you get hacked. One morning, an advanced strain of ransomware easily sidesteps your free antivirus and starts wreaking havoc. It slithers through your systems and locks you out of everything, from client data to basic Word documents, and encrypts it behind a paywall, demanding $50,000 in Bitcoin or you'll lose access to all of it — forever.

You couldn't make room in your budget for a robust cyber security solution. Well, how does that $50K ransom strike you?

This may sound like nothing more than a horror story, but in reality, this happens to business owners all over the world each and every day. An IBM security study from last December discovered that over half of businesses surveyed had paid over $10,000 in ransomware payoffs, with 20% paying over $40,000. And that's not even including the millions of dollars of damage caused by other forms of malicious software every year.

The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology.

Think of it this way. Say, with your free antivirus, you're "saving" $100 a month. Lo and behold, a virus manages to punch its way through and causes chaos throughout the company server. Even if you're lucky and it isn't ransomware, by the time you've managed to expunge the stubborn virus from your business, you'll have put in countless man-hours, guaranteed to cost you more than that $100 a month. Instead of throwing those thousands of dollars down the drain, you'd be better off giving each of your employees a $1,000 bonus!

Free antivirus software, giveaway cyber-protection, or a $5 firewall seems like a great idea, until a hacker cuts through your company's defenses like a warm knife through butter. These guys love when they see these outdated, cheapo barriers guarding your priceless data — those are the paper-thin defenses that keep hackers in business.

You wouldn't buy a rusty, secondhand old lock for your house, so why are you installing primitive cyber security software to protect your most precious company resources?

In today's world of rampant cybercrime, it's inevitable that somebody will come knocking at your digital door. When that day comes, do you want a free piece of software that you saw on LifeHacker, or a tried-and-tested, up-to-the-minute, comprehensive security solution?

Don't be shortsighted and risk everything just to save a quick buck. Invest in your company's future, and protect yourself with the most powerful tools on the market. Call us at (561)969-1616 and allow our skilled consultants assist you with your network security.

"The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology."

PalmTech's Free Executive Brief Reveals The Top 10 Ways Hackers Get Around Your Firewall & Antivirus To Rob You Blind

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.

To Claim Your Free Report, Visit
www.palmtech.net/10ways/

Shiny New Gadget Of The Month:

Picture Keeper Connect, The Best Way To Back Up Photos On The Go

Nothing feels worse than having to delete an old favorite to make room for some new photos. The Picture Keeper Connect solves both of these issues, providing easy-to-use backup for your phone or tablet.

The Picture Keeper Connect, which looks a lot like a conventional flash drive, is designed specifically to back up photos, videos and contact information with just a couple of button presses. It plugs into your phone and gets to work. Even better, it can do all of this without the need for WiFi or network connection. It keeps your photos in their designated album, meaning you won't end up with a cluttered mass of photos when you transfer them to a new device.

Simple, functional, and portable, the Picture Keeper Connect is a must for any avid smartphone photographer.

A Diverse Team Is More Productive

Everyone knows the saying, "If you build it, they will come," from the 1989 film Field Of Dreams. Well, the same rule applies to the type of work environment you create, and, as a result, how diverse your team becomes.

Diversity may not happen overnight, but you can be sure that a diverse team means a broader range of perspectives brought to the problem-solving table. When employees feel accepted and comfortable in their workplace, you can expect them to take more chances on out-of-the-box thinking and creativity, not to mention increased productivity.

But you can't expect your employees to feel safe expressing their identities, and thus their ideas, if you don't first create an inclusive environment for them. But how do you create a space in which your team feels safe drawing from their unique perspectives?

One way to make your employees feel more visible and heard is through diversity networks, groups that come together based on shared identities, like single moms, veterans, LGBTQ individuals, Asian-Americans, the disabled or Latinx. These networks help individuals support and learn from one another, share resources and discuss the challenges and stereotypes facing this facet of their identity and how to address them. If you're worried that this could divide the office more than unite it, don't be. These networks empower individuals to share their experiences with the broader team, allowing everyone to learn from each other.

You also need to make sure you allow opportunities for team members to express themselves. The quickest way to make an employee feel uncomfortable and unaccepted is to have their co-workers interrupt or speak over them. Provide moments for individuals to talk about the projects they are working on, their goals and their struggles.

Diversity training can be helpful in the office. The fact is, everyone has a bias, and it's usually subconscious. Diversity workshops can be a great way to unpack our biases and privilege. Being able to listen and empathize is a vital skill in any business setting, and will improve not only communication between your employees, but their customer service skills as well. A diversity workshop should not be a lecture, but rather an opportunity for honest conversation and learning.

Institute an open-door policy so that your employees feel safe coming to you and their other bosses about issues of discrimination, sexism, racism, homophobia and more. First and foremost, listen. Don't invalidate their experiences by immediately questioning them or taking a side in the conflict. This, plus literally keeping your door open as often as possible, will instill a feeling of trust in your office.

Show that diversity is important to you by hiring employees who come from a variety of backgrounds. Your work team should ideally represent the full diversity of your customer base, enabling them to relate and appeal to your clients on a personal level. Representation also works as a strong motivator. When individuals can see themselves in their role models — bosses, podcast guests, interviewees, etc. — they'll be more likely to imagine higher goals for themselves.

MIKE MICHALOWICZ started his first business at the age of 24, moving his young family to the only safe place he could afford-a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com/

Law firm's automatic deletion of spam emails is blamed for failure to file timely appeal

A Florida law firm's failure to appeal an order assessing attorney fees doesn't constitute excusable neglect when its email system apparently perceived the order to be spam and erased it, a Florida appeals court has ruled.

The Aug. 10 decision by Florida's First District Court of Appeal is being touted as a cautionary tale for lawyers, Law.com (sub. req.) reports.

The law firm, Odom & Barlow, had asked the trial judge to re-enter the order assessing attorney fees so it could file an appeal within the deadline. After a hearing that included testimony by information technology experts, the trial judge refused. The appeals court affirmed.

Among the experts who testified was William Hankins, who said he provided IT consulting for Odom & Barlow beginning in 2007. He said the law firm's email system was configured to drop and permanently delete spam emails without alerting the recipient.

Hankins recommended against this configuration because the email system could identify legitimate emails as spam. He recommended that the firm use a third party to handle spam filtering, but the firm rejected the proposal because it didn't want to spend the money.

Hankins said that, in 2015, he recommended the firm get an online backup system for emails that would cost between $700 and $1,200 a year, but the firm rejected the advice. Hankins said he quit working for the firm because it rejected the recommendations.

Other experts said the order assessing attorney fees was apparently received by the law firm's server, and could have been deleted as spam as a result of the email system's configuration.

"Based on this testimony," the appeals court said, "the trial court could conclude that Odom & Barlow made a conscious decision to use a defective email system without any safeguards or oversight in order to save money. Such a decision cannot constitute excusable neglect."

The amount of attorney fees at stake is as high as $1 million, the Pensacola News Journal reports.

The law firm didn't immediately respond to a request for comment.

Author: Debra Cassens Weiss, ABA Journal
www.abajournal.com

Equifax's Leak: Lessons Learned

EQUIFAX

No business owner wants their customers' data leaked, but no matter how well your prevention plan is, the unexpected can happen. And when it does, what will determine the fate of your business is how well you respond to it. So before you start planning an incident response, read the following story and recite this: Don't walk in the footsteps of Equifax.

Read More Here: www.palmtech.net/equifax-lessons/