PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions March 2017

Is Your Disaster Recovery Plan Up To Par?

No matter how much we analyze network activity, or how many cyber-security conferences we attend, nothing educates us like the missteps of real-world businesses. Learning from example is by far the best way to beef up any disaster recovery plan (DRP), and the recent audit of a state government office gifted us plenty of useful information.

Visit www.palmtech.net/disaster-recovery-plan for our three takeaways from the report.

March 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.

"Lucky Charm" Keeps Hackers Out

Ralph's been a good employee for you. Shows up on time. Gets the job done. Doesn't hassle anybody.

He's also a porn addict. When nobody's looking, he's visiting sites – on your network – that you'd be appalled to see. IF…you knew about them. Without careful monitoring and filtering, this kind of Internet use on your network can remain hidden. Shocking? Hard to believe it could happen at your company? A survey by International Data Corporation (IDC) revealed that 70% of all web traffic to Internet pornography sites occurs during the work hours of 9 a.m. to 5 p.m. Ralph's little visits may seem harmless, but they're adding a serious level of risk to the financial health and security of your company.

Here's how. A visit to an adult website can be tracked. And if a logged-in user's identity is leaked, it can be embarrassing, to say the least, to that user. The user may even become a victim of "sextortion" or blackmail. Just ask any of the people who used Ashley Madison, a dating site for illicit affairs. When the site was hacked, users were suddenly at risk of having their indiscretions revealed. This gives cybercriminals a powerful lever to pressure an employee into revealing sensitive company data. Considering that 60% of security breaches start from within the company, you have to wonder what someone at risk of being exposed might do to keep their little secret, well…secret.

Let's face it, if you're not carefully monitoring and managing how your network is being used, your company's data could be in serious jeopardy.

Content Filtering In Today's Web 2.0 World

Whether you're already monitoring user activity on your network or not, you need to stay vigilant about evolving risks. And content filtering is key. If your business is like many,

continued on page 2

you may already be doing some filtering. But is it enough? As technology evolves, hackers drum up ever stealthier ways to invade your network.

Cloud-based filtering, for example, becomes a must when mobile devices tap into your network. The old concept of a static, location-based "firewall" just doesn't cut it anymore when your staff goes mobile.

Then there's social media. It's like a big window into the personal lives of your personnel. It lets cybercriminals "case the joint" before breaking in. For instance, when users log in to a personal Facebook account at work and talk about vacations, favorite hangouts or weekend activities, hackers can use that information for social engineering and other ploys.

The number of ways your network is exposed to potentially damaging content grows daily. It's no wonder that 90% of companies and government agencies surveyed by IDC detected computer security breaches within the previous 12 months. Eighty percent of those organizations acknowledged financial losses due to these breaches. With odds like that against you, an up-to-date content filtering system could well be THE "Lucky Charm" that keeps your company, and your data, safe from all kinds of harm.

FREE Web And E-mail Usage Audit Instantly Reveals If You Have A Problem

***FREE Web And E-mail Usage Audit Instantly Reveals If You Have A Problem**

If you'd like a snapshot of where your employees are going online and how much time they're spending surfing the net on non-work-related activities, I'd like to offer you a *FREE Internet And E-mail Usage Audit worth $375. At no cost or obligation on your part, we'll come by and install a special diagnostic program that will expose lurking threats due to inappropriate employee use of websites, e-mail and instant messaging.

I'm making this offer because I'd like to give you a bite-sized sample of our extraordinary customer service and proactive approach to protecting you and your organization. And to be perfectly clear, no matter what we may find during your audit, you are under no obligation to buy anything or ever use our services again.

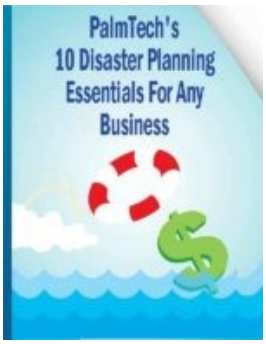
However, there is a catch: we'd like to help every company in the West Palm Beach area eliminate this risk, but we're only able to perform 5 audits per month. Call **(561)969-1616** or email us at info@palmtech.net now, while you're thinking of it. The five minutes you invest could save your company thousands of dollars in lost productivity, potential lawsuits and company resources.

Let's not let your company become yet another statistic, hemorrhaging cash as a result of a destructive cyber attack. Call me **TODAY** at (561)969-1616 or e-mail me at info@palmtech.net and let's make sure your systems are safe. I'll provide you with a Cyber Security Risk Assessment to check for and safeguard against any points of entry for an attack. This service is FREE, but DO NOT RISK WAITING: contact me NOW before the next scam puts your network at risk.

**Offer valid to qualified prospects with 15 or more computers and a minimum of 1 server.*

PalmTech's 10 Disaster Planning Essentials For Any Business

During this time of year, the threat of fire, flood, severe storms, water damage from office sprinklers, and even theft is very real.



One of the most valuable assets for any company is its data. Hardware and software can easily be replaced, but a company's data cannot!

Don't lose everything you've worked so hard to achieve in an instant! PalmTech's report, **"The 10 Disaster Planning Essentials for Any Business"** will reveal important planning strategies you should have in place now to protect yourself from common data-erasing disasters including natural hazards, human error, cyber criminals, hardware failure, software corruption and other IT failures.

Visit www.palmtech.net/data-protected/ to download this FREE report!

Shiny New Gadget Of The Month:

Handheld? Console? No, It's...Switch!

Nintendo's long-awaited new gaming platform Switch should be available any day now, if it isn't already. It combines the best elements of handheld games with a home console. Handheld, the gamepad is the screen. Slip it into its dock and it plays on your TV.

The gamepad comes with two detachable "Joy-Cons." One player can hold a Joy-Con in each hand, two players can each take one, or bring in more Joy-Cons and multiple people can play.

If you're on the go, pull out the "kickstand" on the back of the gamepad and prop it up on an even surface for easy viewing. There's a slot on the side for game cards and a USB-C port for quick charging.

Because it has greater processing power than the Wii U, you'll have no trouble playing Legend of Zelda: Breath of the Wild, Super Mario and a host of your other favorite Nintendo games.

Solve It By Sundown

The Internet has revolutionized the computer and communications world like nothing before. This worldwide broadcasting system can disseminate information without regard to geographic locations at the speed of a "click," and therein lies a BIG PROBLEM.

The speed of a "click" has now conditioned us to how fast we expect things. If you want a book, you just download it (CLICK). If you want a movie, you just download it (CLICK). If you want a song, you just download it (CLICK). If you want information about something, you just go to Google, type in the info you need and CLICK. We are all being conditioned to getting INSTANT service and information. That being said, it should be no surprise to you that your customers are becoming more and more demanding at getting whatever they want…NOW!

Right now, there are some of you who have already received a few text messages while you are reading my article, and people are expecting an instant response. There is no turning back or slowing down when it comes to technology; there is only speeding up and moving forward. Therefore, the companies that will succeed are doing everything they can to please their customers in a manner their customers expect…which happens to be…NOW!

I would, therefore, recommend a simple slogan, mantra or motto for all employees of your company to live by…Solve "IT" by Sundown…because if you don't, you have just opened the door for your competitor to do so. I used to work with an IT company that sent out my weekly articles; if I ever had a problem with their service, their standard response was "We will get back to you with a resolution in 72 hours." The third time that happened I changed companies. My new IT company had me up and running in one hour and I have been working with them for years.

Anytime you push off a customer to fix something tomorrow (or in 72 hours), you are giving them the opportunity and incentive to go find someone who would be willing to fix the problem today. Your customer is thinking, "If they can fix it tomorrow, then why can't they fix it today?" Now, sometimes you don't have the part(s) or person available to fix it today and you tell the customer that. Well, my question to you is this: Does your competitor? Remember the Internet: a few typing strokes and clicks on a computer, and I will have a list of your competitors available to ask that question, and if they can fix it, YOU ARE GONE, FINISHED, TOAST.

The brilliant man Benjamin Franklin once said, "Don't put off until tomorrow what you can do today." I don't believe Mr. Franklin ever envisioned the Internet, but he sure understood how to be successful. If you want to set your company apart from your competition, then I would do everything I could to establish a culture that understands…

WHEN AT ALL POSSIBLE – SOLVE IT BY SUNDOWN.

Robert Stevenson is a highly sought after, internationally known speaker. He is the author of the best-selling books "How to Soar Like An Eagle in a World Full of Turkeys" and "52 Essential Habits For Success". Robert is a graduate of the Georgia Institute of Technology (Georgia Tech) and is a former All-American Athlete. He started his first business at 24 and has owned several companies. Robert has international sales experience dealing in over 20 countries, and his client list reads like a Who's Who in Business. He has shared the podium with such renowned names as Generals Colin Powell and Norman Schwarzkopf, Former President George H.W. Bush, Anthony Robbins and Steven Covey. www.robertstevenson.org

How Can You Go From Reactive IT to Preventive IT?

Shopping around for a managed IT services provider is tough. You're looking for a business to manage extremely complex and delicate technology, so they can't be expected to get into the nitty gritty details of DNS-layer security, intrusion prevention systems, and encryption in their marketing content. But one thing does need clarification: What exactly are "proactive cyber-security" measures?

Understand the threats you're facing

Before any small- or medium-sized business can work toward preventing cyber-attacks, everyone involved needs to know exactly what they're fighting against. Whether you're working with in-house IT staff or an outsourced provider, you should review what types of attack vectors are most common in your industry. Ideally, your team would do this a few times a year.

Reevaluate what it is you're protecting

Now that you have a list of the biggest threats to your organization, you need to take stock of how each one threatens the various cogs of your network. Map out every device that connects to the internet, what services are currently protecting those devices, and what type of data they have access to (regulated, mission-critical, low-importance, etc.).

Create a baseline of protection

By reviewing current trends in the cyber-security field, alongside an audit of your current technology framework, you can begin to get a clearer picture of how you want to prioritize your preventative measure versus your reactive measures.

Before you can start improving your cyber-security approach, you need to know where the baseline is. Create a handful of real-life scenarios and simulate them on your network. Network penetration testing from trustworthy IT professionals will help pinpoint strengths and weaknesses in your current framework.

Finalize a plan

All these pieces will complete the puzzle of what your new strategies need to be. With an experienced technology consultant onboard for the entire process, you can easily parse the results of your simulation into a multi-pronged approach to becoming more proactive:

- Security awareness seminars that coach everyone -- from receptionists to CEOs -- about password management and mobile device usage.
- "Front-line" defenses like intrusion prevention systems and hardware firewalls that scrutinize everything trying to sneak its way in through the front door or your network.
- Routine checkups for software updates, licenses, and patches to minimize the chance of leaving a backdoor to your network open.
- Web-filtering services that blacklist dangerous and inappropriate sites for anyone on your network.
- Antivirus software that specializes in the threats most common to your industry.

"Serendipity is up, fluke is doing well, but I'm a little concerned about our dumb luck."

As soon as you focus on preventing downtime events instead of reacting to them, your technology will begin to increase your productivity and efficiency to levels you've never dreamed of. Start enhancing your cybersecurity by giving us a call at (561)969-1616 for a demonstration.

Techadvisory.org