PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions May 2016

Please Welcome Tina Mike To The PalmTech Team!

We would like to introduce Tina Mike, Senior Account Manager, as the newest member of our team at PalmTech Computer Solutions.

Tina brings more than 25 years of knowledge and experience in technology in addition to the management of business accounts.

We are confident that she will be an asset to both our company and our clients.

Please join us in welcoming Tina to the PalmTech family!

MAY 2016

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

Quote of the Month:

"Whether You Think You Can Or Think You Can't, You're Right."

- Henry Ford

10 Things You Must Do Now To Prevent A Costly Data Disaster

In less than 60 seconds, you are about to learn 10 things that could save you days – or even weeks – of downtime, not to mention the undue stress on your company, and potentially thousands of dollars lost, due to a data disaster…

Use this article as your checklist in a conversation with your IT company to assure that your business has the right plan in place to get back up and running quickly if and when disaster strikes.

1. **Keep a written plan.** Simply thinking through in ADVANCE what needs to happen when things go south on you, and documenting it, can go a long way toward getting your network back up and running quickly if it gets hacked, flooded or compromised by human error or equipment failure.

   Outline the types of disasters that could happen, and a step-by-step recovery process. Be sure to include a budget, what to do, who should do it and how. Store printed copies along with key contact information and login details for essential websites 1) in a fireproof safe, 2) off -site at your home, 3) at each key employee's home and 4) with your IT consultant.

2. **Hire a trusted professional to help you.** Trying to recover data after a disaster without professional help is business suicide. One misstep can result in weeks of downtime, or permanent data loss. To improve your odds of a quick recovery, work with a pro who has experience in both setting up your plan and helping you recover when a loss occurs.

3. **Have a communications plan.** What if your employees can't access your office, e-mail or phone system – how should they communicate with you? Make sure your plan details the alternatives, including MULTIPLE ways to stay in touch.

continued on page 2

4. **Automate your backups.** THE #1 cause of data loss is human error. If your backup system depends on a human being doing something, it's a recipe for disaster. ALWAYS automate your backups so they run like clockwork.

5. **Keep an off-site backup copy of your data.** On-site backups are a good first step, but if they get flooded, burned or hacked along with your server, you're out of luck. ALWAYS maintain a recent copy of your data off-site.

> *"It's critical to keep your network patched, secure and up-to-date."*

6. **Be able to access and manage your network remotely.** You and your staff will be able to keep working if they can't get into your office. Your IT manager or consultant can quickly handle an emergency or routine maintenance. And you'll love the convenience!

7. **Image your server.** Storing your *data* off-site is great – but bear in mind, if your *system* goes down, the software and architecture that handles all that data must be RESTORED for it to be of any use. Imaging your server creates a replica of the original, saving you an enormous amount of time and energy in getting your network back in gear. Best of all, you don't have to worry about losing your preferences, configurations or favorites.

8. **Document your network.** Network documentation is simply a blueprint of the software, data, systems and hardware that comprise your company's network. Let your IT manager or consultant create this for you. It'll save you time and money in the event your network needs to be restored.

It also speeds up everyday repairs and maintenance on your network when technicians don't have to waste time figuring out where things are and how they're configured. Plus, it may help with insurance claims in the event of losses due to a disaster.

9. **Maintain your system.** While fires, flooding and other natural disasters are certainly a risk, it's ever more likely that you'll experience downtime due to a virus, worm or hacker attack. That's why it's critical to keep your network patched, secure and up-to-date. And don't forget: deteriorating hardware and corrupted software can wipe you out. Replace and update them as needed to steer clear of this threat.

10. **Test, test, test!** If you're going to go to the trouble of setting up a plan, at least make sure it works! Hire an IT pro to test monthly to make sure your systems work properly and your data is secure. After all, the worst time to test your parachute is AFTER you jump out of the plane.

Need help getting this implemented? Contact us by June 10th, 2016 at (561) 969-1616 or info@palmtech.net for a **FREE Backup And Disaster Recovery Audit.**

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

Win Free Coffee and an iPad!

Don't Keep Us a Secret!
Recommend PalmTech to Your Professional Contacts.

Details here:
Www.PalmTech.net/referral-program/

Ransomware Threats Continue to Loom

Government facilities, hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—just a few of the entities impacted recently by ransomware, a devious type of malware that locks valuable data files and demands a ransom to release them.

The inability to access the important data these kinds of organizations keep can be devastating in terms of the loss of sensitive information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation.

During 2015, law enforcement saw an increase in these Ransomware attacks, particularly against organizations because the payoffs were higher. And if the first three months of this year are any indication, the number of ransomware incidents—and the ensuing damage they cause—will grow even more in 2016 if individuals and organizations don't prepare for these attacks in advance.

In order to mitigate the risks associated with Ransomware attacks, organizations must invest in the proper security measures:

1) adopt robust technical prevention controls
2) Train and retrain employees on the threats that exist and identify the steps that should be taken when a threat has been discovered
3) Backup files regularly and keep a recent backup off-site.
4) Don't enable macros - Some ransomware is distributed in Office documents that trick users into enabling macros.
5) Use caution when opening unsolicited attachments.

Call PalmTech at (561)969-1616 for a Security & Backup Audit, which will assess your company's overall network health to review numerous data-loss and security loopholes. Don't risk being a victim. Be certain your business, your reputation and your data are protected.

Conquering Connecting

"Everyone looks so much better when they smile." – Jimmy Fallon, host of the legendary *The Tonight Show*

What a meteoric ride Jimmy Fallon has had to the top!

How did this son of an IBM machine repairman get to the chair once occupied by maybe the most legendary figure in comedy TV for 30 years straight, Johnny Carson?

He did it through exceptional networking.
In the span of about five years, Jimmy went from a *Saturday Night Live* alum, unsuccessfully navigating Hollywood, to a late-night star and host of NBC's *The Tonight Show*, one of the most respected franchises in entertainment. This did not happen by accident…

Fallon's meteoric rise is partly due to his intense focus on developing relationships with people who could advance his career.

Another key? Fallon worked his butt off.
While still a computer-science major at Albany's College of Saint Rose, he performed comedy at small clubs and obsessed about the comedy industry.

Through a connection with his former employer at a New York alternative newsweekly, his audition tape reached Hollywood agent Randi Siegel, who had ins with the crowd at *Saturday Night Live*.

Siegel found 21-year-old Fallon's performance to be charmingly amateur, but she could see that he was naturally talented. She gave him a call and was surprised to hear, after introducing herself, "Randi Siegel! I know who you are!"

Randi was so impressed by his knowledge of the comedy industry and enthusiasm that she agreed to take him on as a client.

With Siegel's connections, Fallon was able to eventually get hired as a cast member with *SNL* in 1998.

At *SNL* he developed the relationship that would define his career.
The show's creator, Lorne Michaels, is so powerful and respected in the industry that cast members are often intimidated by him. As a rookie, Fallon was no different, but he wanted to befriend Michaels. So after every show, he went over to Michaels and thanked him for the show.

Michaels developed a rare friendship with Fallon. Following the drama of Conan O'Brien's short stint as host of *The Tonight Show*, Michaels decided that his trusted Fallon would take the renowned position.

Fallon made a point of connecting with former *Tonight Show* host Jay Leno and would ask for advice. Leno said, "Most people in show business think they know everything. They don't really listen to the other person. 'Respectful' is the best word I can use for Jimmy."

His approach worked.
Since starting in February 2014, Fallon has attracted around 4 million viewers each night, with a much higher share of the 18-49 demographic than his predecessor.

What Fallon did is a) he worked hard (let's not forget that), and b) he networked brilliantly by asking questions of others, listening, acting on their advice, showing gratitude and being a genuinely good human being.

So, who are three connections you dream of networking with in order to boost your success?

Darren Hardy is the visionary force behind SUCCESS magazine as the Founding Publisher and Editor, and is the New York Times and Wall Street Journal bestselling author of what has been called "the modern day Think and Grow Rich": The Compound Effect—Jumpstart Your Income, Your Life, Your Success (www.TheCompoundEffect.com) and the world-wide movement to onboard 10 million new entrepreneurs through his latest book The Entrepreneur Roller Coaster--Why Now is the Time to #JoinTheRide (www.RollerCoasterBook.com). Access Darren: www.DarrenHardy.com and get free daily mentoring: www.DarrenDaily.com.

Avoid Landmines & Hefty Fines That Can Result From HIPAA Non-Compliance

Small and medium businesses will find themselves faced with several adverse repercussions for noncompliance with HIPAA rules. Businesses that have never been confronted with HIPAA concerns before are now discovering that the guidelines are not limited to "Covered Entities" such as doctors, dentists, hospitals, clinics, pharmacies, insurance companies, and labs, but encompass *any* business, i.e. legal firms and accountants, that may perform certain functions or activities involving the use or disclosure of protected health information (PHI) on behalf of a Covered Entity. PHI includes medical history, lab results, insurance information, social security numbers, records, and various other types of personal data. In order to remain HIPAA compliant, Covered Entities must have Business Associate Agreements with any third party contractors that have been given access to PHI. If a vendor qualifies as a "Business Associate" but fails to comply with HIPAA regulations, they will meet serious penalties, for example a fine of $1.5 million.

Not only do these business associates need to comply with HIPAA, they must require their own subcontractors that have been given access to PHI do the same. For instance, law firms are required to review their contracts with cloud service providers, expert witnesses and others to ensure those organizations are HIPAA compliant. The chain of liability extends infinitely.

HIPAA compliance is the topic of numerous conversations since several healthcare data breaches have occurred as a result of stolen devices, unauthorized access, miscellaneous errors, or hacking. According to the Office of Civil Rights (OCR), there were over 253 healthcare breaches which totaled more than 112 million records in 2015.

Such regulations are extremely complex. Firms that handle PHI should consider turning to partners who not only have a thorough understanding of the risks but have the resources to ensure all protocols are being met. This is particularly true for smaller firms that may lack some of the on-staff compliance specialists that larger firms retain.

By working with PalmTech, a trusted and experienced partner, businesses can avoid cyber-risks while improving their peace of mind, allowing them to focus on their client needs. Contact PalmTech at (561) 969 -1616 or info@palmtech.net before June 10th, 2016 to schedule a **HIPAA Evaluation FREE** for your organization!

Remember - ignorance is no excuse. As of December of 2015, only 14% of legal firms were in compliance. Doing nothing is not an option. Florida Bar Ethics Rules REQUIRE HIPAA compliance for personal injury, elder law, medical malpractice, and any other practice that accesses sensitive information/protected health information. Call us today for assistance.