PALMTECH
I.T. SOLUTIONS FOR BUSINESS

THE PALMTECH TIMES

Inside this Issue:

© MARK ANDERSON, WWW.ANDERTOONS.COM

August 2016

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.

Betting The Farm Your Backups Are Safe?

It's only natural that when you hear of a disaster you think it couldn't happen to you.

That's why, even though we're told constantly that we should diligently maintain a working backup recovery system because all our company's data could be lost in an instant, we tend to brush off the advice.

Yet disasters do happen when you least expect them, and they can happen to anyone. So to illustrate the importance of staying on top of your data recovery system, here are three tales of "data gone wrong." After all, there's nothing quite like a good horror story to inspire action!

Toy Story 2: Gone!
One morning in 1998, the animators at Pixar Studios working on *Toy Story 2* noticed that Woody's hat started disappearing. Then his boots… Then all of Woody – gone! Other characters started disappearing too.

A rogue command in their system had started wiping out data. No problem, the team thought, as they pulled out the backups.

Unfortunately, the backups were bad and only had data from 10 months ago.

Luckily, one of the project leaders who'd just had a baby had recently asked to have a copy of the film installed at her house. So they drove to her house and escorted her computer back to the studios "like an Egyptian Pharaoh." And as we now know, *Toy Story 2* was saved.

Moral: It's not enough to simply run backups. You need to periodically check to make sure the data is actually getting backed up and nothing is corrupted.

46,000 Insurance Customer Records: Lost!
In 2010, Zurich Insurance announced it had lost a backup tape containing confidential data from 46,000 customer records as it was being transferred from one site to another. To make matters worse, it was later revealed that it took a full year for their headquarters to learn that the tape was missing.

While there was no evidence that the data had fallen into the wrong hands, it was not encrypted and therefore easily accessible by anyone in possession of the tape. The company was slapped with a £2.3 million fine from the British Financial Services Authority.

Moral: If your backups are physical, make sure they're transported and stored securely in a location away from your computer. And regardless of whether your backups are physical or in the cloud or both, make sure they are encrypted with high-level security.

Why MegaPetCo Closed Their Doors

The fast-growing set of chain stores MegaPetCo had refused to upgrade their IT system to one that could handle their needs. One day a systems developer accidentally programmed a query that wiped out their entire database. All of a sudden, operations ground to a halt; from sales to payroll to purchasing

> *"Everything had been tied into that one database. And no backup."*

and reporting, everything had been tied into that one database. And no backup.

They tried to sue their ISP, but between recommendations to upgrade and failure to do so, the lawsuit was dropped. Three months later, MegaPetCo filed for bankruptcy.

Moral: Just because your data is in the cloud or hosted somewhere else do not assume it is being backed up. Even if it is, you should still be backing up cloud data to your own network or make sure it is going to an account that you have access to in case something happens to your vendor that is hosting your data. And as we always recommend, make a backup before any major changes-including mass deletions.

Why Take A Chance That Your Backups Are Safe? Our FREE Data Recovery Audit Will Help You Know For Sure!

The effects of a data disaster run the gamut from minor annoyance to a death knell for the organization it

happens to. We don't want that for you. That's why **until August 31st**, we're offering our complete audit, normally valued at $497, **free*** to businesses in the West Palm Beach area.

At no charge, our data security specialist will come on-site and audit your current data backup and security procedures and determine whether your current system can guarantee you a fast, safe and full recovery of your data.

Depending on what we find, we'll either give you a clean bill of health or reveal gaps in your data backup system that could prove catastrophic. Then, if appropriate, we'll provide you with an action plan for further securing your data with our **state-of-the-art computer hard drive backup and disaster recovery solutions.**

Call (561) 969-1616 TODAY and let's make sure your company isn't betting the farm on a flawed recovery system.

*Offer valid for qualified prospective clients with 15 or more computers and a minimum of 1 server.

Is It Time For Cybersecurity Planning?

The time to start planning for a security threat isn't during a virus outbreak or immediately after you discover funds transferred within your banking accounts. Decisions and judgments made during this time are typically driven by emotion and not facts. The time to make those cyberthreat plans is now.

Things to consider when you're planning:

- Physical access to your building(s)
- What to do with lost or stolen mobile devices
- PCI (payment card industry) compliance requirements
- Data-breach incident response

- Threat monitoring

That's where we are here to help! Give us a call and we'll be glad to help you evaluate your "cybersecure" plan.

There are great resources out there for businesses that just don't know where to start with cybersecurity. Take a look at http://www.fcc.gov/cyberplanner for a customizable guide on where to get started with operational and organizational planning.

If you need assistance, don't hesitate to contact us at (561) 969-1616 or email us at info@palmtech.net.

Shiny New Gadget Of The Month:

A Great Night's Sleep In The Palm Of Your Hand

The techno-geeks over at Hello Inc. have just released Sense, a device that helps you wake up feeling great. A tad smaller than a baseball, this little sphere sits on your nightstand next to your bed and monitors conditions in your room while you sleep. Things like temperature, humidity, light and sound in your bedroom are tracked, along with your body's slightest movements as you sleep. It pairs with your smartphone so you can see patterns and change conditions in your room to get the best night's sleep possible. Sense can play any number of soothing sounds to help you drift off to sleep. Then, when it's time to rise and shine, it gently wakes you up at the best time in your sleep cycle. It's priced at $129, and you can find it at hello.is and other online retailers.

A Flexible Business Equals a Business of the Future

We hear it all the time - "there's an even newer technology out!" "A brand new platform was released that is leagues ahead of the competition!" "This new program makes every other program obsolete!" Keeping up with all the new technologies is imperative. It's exciting and for the first time in history, how you view technology and how your business approaches it has an enormous impact on how successful you are. Here are the three most important aspects of establishing a business able to keep up with the changing technologies and practices.

Falling behind the times is not an option. Staying up with the newest technologies is a must. If you let your business get behind in the technology it needs to stay competitive, playing catch up could be disastrous. As the competition continues to move forward and they can offer services more efficiently, at better prices, with better results, you lose. Staying up to date with the latest and best technology provides a huge step up in the business world.

Who you hire can have a huge impact in how well your business adapts to changes in technologies. To have a flexible business, you need flexible staff members. This may be harder to do since you never know how someone will perform until you see them in action, but if you can establish a culture within your company of flexibility and

modern thinking, your employees will step up to the plate and perform. Make professional development a requirement and you'll create a staff of flexible, knowledgeable employees who can handle the rapid changes coming their way.

Think of the last time you sat down to work on your business strategy and five-year plan. Did a five-year plan seem less relevant than it did even a few years ago? As we continue to progress and grow, long term plans are becoming obsolete. To achieve the flexibility your business needs, you need to have the mindset that immediate, constant adjustment is what is required. By switching up the priority level of each staff member, team-based goals can be realized quickly and efficiently. Less focus is necessary on the future goals and more placed on the immediate daily incidents.

By creating a flexible company, you'll be able to better keep up with the new technology demands and the changing face of business. You'll gain a step up over the competition and place yourself in a position for growth. A flexible, adaptable business is more likely to achieve success in our evolving business world.

If you have questions or need recommendations on technology suited for your business, please contact us at info@palmtech.net or at **(561)969-1616**.

Which Type of Organizations are 114 Times More Likely To Suffer Ransomware Attacks??

- Healthcare organization's computer networks are 114 times more likely to suffer ransomware attacks than those at financial institutions, and 21 times more likely than schools and universities, CSO reports.

- The sobering statistic surfaced in a new report by security firm Solutionary, which experienced 88% of ransomware infections in the first six months of 2016 despite having healthcare account for just 7.4% of its client base.

- In early July, HHS' Office (US Department of Health & Human Services) for Civil Rights issued draft guidance to help healthcare organizations tackle ransomware threats head on. The assistance reinforces HIPAA-required activities which organizations can use to prevent, detect, contain, and respond to threats.

"The most important steps in protecting your company's and your customers' data from the growing malicious ransomware onslaught are ensuring that you have a robust backup and recovery process, and that your security software is up-to-date and able to detect the most recent ransomware variants," Rob Kraus, director of research for Solutionary's SER team, said in a statement. "As the threat continues to evolve, it will be crucial for organizations to have defined incident-response procedures and proper detective and preventive controls in place to reduce ransomware's impact."

Many of the healthcare organizations who have experienced a data breach in 2016 have been due to ransomware. Hollywood Presbyterian Medical Center, for instance, in California, was locked out of its EHR for a week. Providers were forced to revert to pen and paper until the decision was made to pay hackers $17,000.

PalmTech can assist with the protection of your company and client data. Our skilled security team will assess your network to determine any vulnerabilities that may exist, then work out a plan to secure those entry points or weaknesses. In addition, if necessary, we will help ensure you are following the required HIPAA regulations.

Keep in mind - *even if you don't fall under the "medical facility" category, you are STILL required to follow HIPAA guidelines if your company handles protected health information (PHI). For instance, legal firms, insurance companies, chiropractors, schools, non profit organizations, and optometrists are a few types of businesses that must be HIPAA compliant.*

Call us at **(561)969-1616** or email us at **info@palmtech.net** to discuss.

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/

© Randy Glasbergen
glasbergen.com

"We're implementing new security standards in the office, so don't forget to use the ecret-say ode-cay!"