PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions October 2016

Inside this Issue:

October 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.

Could One Tiny Leak Wipe Out Your Entire Company?

Things were going great at Michael Daugherty's up-and-coming $4 million medical-testing company.

He was a happy man. He ran a good business in a nice place. His Atlanta-based LabMD had about 30 employees and tested blood, urine and tissue samples for urologists. Life was good for this middle-aged businessman from Detroit.

Then, one Tuesday afternoon in May 2008, the phone call came that changed his life. His general manager came in to tell Daugherty about a call he'd just fielded from a man claiming to have nabbed a file full of LabMD patient documents. For a medical business that had to comply with strict federal rules on privacy, this was bad. Very bad.

It turned out that LabMD's billing manager had been using LimeWire file-sharing software to download music. In the process, she'd unwittingly left her documents folder containing the medical records exposed to a public network. A hacker easily found and downloaded LabMD's patient records. And now the fate of Michael's life – and his business – were drastically altered.

What followed was a nightmarish downward spiral for LabMD. Not one to go down without a fight, Michael found himself mired in an escalating number of multiple lawsuits and legal battles with the Federal Trade Commission and other regulators investigating the leak.

Finally, in January 2014, exhausted and out of funds, his business cratering under constant pressure, he gave up the fight and shuttered his company.

One tiny leak that could have easily been prevented took his entire company down. Could this happen to you and your business? Let's take a look at four fatal errors you MUST avoid, to make sure it never does:

Have you developed a false sense of security? Please, please, please do NOT think you are immune to a cyber-attack simply because you

continued on page 2

are not a big company. The fact is, whether you have 12 clients, or 12,000 clients, your data has value to hackers. A simple client profile with name, address and phone number sells for as little as $1 on the black market. Yet add a few details, like credit card and Social Security numbers, and the price can skyrocket – $300 per record is not uncommon. Being small doesn't mean you are immune.

> *"You MUST remove those accounts without delay."*

Are you skimping on security to save money? Sure, of course you have a tight budget… So you cut a deal with your marketing manager, who wants to work from home at times. He links into the company network with a VPN. If configured properly, your VPN creates a secure and encrypted tunnel into your network. So his device now links his home network into the company network. The problem is, his home cable modem may be vulnerable to attack, an all-too-common issue with consumer devices. Now you have an open tunnel for malware and viruses to attack your network.

Could lack of an off-boarding process put your company at risk? It's crucial to keep a record of user accounts for each employee with security privileges. When an employee leaves, you MUST remove those accounts without delay. An internal attack by a disgruntled worker could do serious harm to your business. Be sure to close this loop.

Have you been lax about implementing security policies for desktop computers, mobile devices and the Internet? The greatest threat to your company's data originates not in technology, but in human behavior. It starts before you boot up a single device. In an era of BYOD (bring your own device), for instance, lax behavior by anyone connecting to your network weakens its security. Your team love their smartphones, and with good reason. So it's tough sticking with strict rules about BYOD. But without absolute adherence to a clear policy, you might as well sell your company's secrets on eBay.

Don't let a tiny leak sink your ship – here's what to do next…

Let us run our complete Network Security Audit for you. We'll send our top data security specialist to your location and give you a complete top-to-bottom security analysis with action plan. This is normally a $397 service. It's yours *FREE when you call now through the end of October.

Don't wait until disaster strikes. Call (561)969-1616 or e-mail me at info@palmtech.net to schedule your FREE Network Security Audit TODAY.

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

FREE HIPAA TRAINING FOR YOUR STAFF

Take the next step toward HIPAA compliance with *FREE HIPAA Training for you and your staff courtesy of PalmTech! Any Medical Office, Law Firm, or Corporation that handles medical records MUST take steps to have all of their employees trained as part of a comprehensive HIPAA compliance strategy. PalmTech has reached an agreement with our HIPAA auditing partner to provide access to their computer-based video training material free for 30 days – plenty of time to get your whole team through the program. Your staff will also be tested and given a HIPAA Certificate upon successful completion of the training course. Call our sales team at (561)969-1616 or email sales@palmtech.net to get your training portal set up today.

**Offer limited to new clients with 15 or more computers whose business deals with or handles medical records.*

Shiny New Gadget Of The Month:

Hololens: Your New Reality?

A game designer sees a moving 3-D image of a living, breathing, mace-wielding ogre – on her desk. She flicks a finger and he turns from side to side, giving her a full view of his outfit and weapons belt.

An architect looks up at the ceiling in a building he's just designed. He waves his hand and reshapes it, allowing more light through. All virtually.

A space scientist designing a Mars rover strolls through the landscape, noting from all sides the position, shape and size of rocks his vehicle must navigate.

Now it's your turn. Put on the new HoloLens by Microsoft, and what do you see? How could you use this cool new augmented reality (AR) tool in your business?

At $3,000 for the developer's version, it may not be an impulse buy. But new AR tools like this will soon be part of your computing world.

Businesses Can Find Improved Backup In The Cloud

For small and medium business owners in flood-prone regions, protecting assets from rising water calls for more than boarding up windows and stacking sandbags - it requires establishing backup processes that enable business continuity in the face of a disaster.

Business continuity (BC) refers to maintaining business functions or quickly resuming them in the event of a major disruption, whether caused by a fire, flood, epidemic illness or a malicious attack across the Internet. A BC plan outlines procedures and instructions an organization must follow in the face of such disasters; it covers business processes, assets, human resources, business partners and more. A Business Continuity plan should include the ability to restore operations in another location if necessary.

Setting up a secondary data location is not an option for many small or medium-sized businesses, such as those in the present flood-ravaged areas of North and South Carolina. That's because, unlike larger enterprises, SMBs often lack the capital and human resources required to first build and then maintain redundant facilities.

Instead, small and medium business owners can turn to cloud-based service offerings to ensure the integrity and availability of data and applications in the wake of a flood.

By delivering failover to the cloud within a predetermined time frame, disaster recovery using cloud based services provides the peace of mind small and medium business owners need.

Such disaster recovery solutions enable employees to access email, web servers and critical applications via the internet, from wherever they are. And many service providers follow a pay-as-you-go model, meaning organizations are charged only for the resources they consume.

Despite the importance — and growing ease — of deploying disaster recovery solutions using cloud based services, some small businesses owners do not prioritize disaster recovery and business continuity planning. After all, considering the demands of the day, future worries seem far away. But is a disaster really so distant? What we have seen with the recent hurricane should answer that.

"Research has shown that due to climate warming increasing the intensity of rain events and sea-level rises, flood events of various severity will become more common," says Mark Hoekzema, chief meteorologist and director of meteorological operations at Earth Networks/WeatherBug. "This could mean more numerous minor floods as well as increasing the potential for a record flood event."

The recent floods demonstrate just how devastating historic flooding can be.

What we can do is minimize the risk and build resilience.

Contact us at **(561)969-1616** or via email at info@palmtech.net for more information on business continuity planning and disaster recovery.

IT Jargon: A Glossary of Cybersecurity Terms

Everyone hates jargon. It's ostracizing and off-putting, but somehow we just keep creating more and more of it. For those who have adopted an "if you can't beat 'em, join 'em" philosophy, we have just the list for you. Let's take a look at some of the most relevant cybersecurity terms making the rounds today.

Malware: For a long time, the phrase 'computer virus' was misappropriated as a term to define every type of attack that intended to harm or hurt your computers and networks. A virus is actually a specific type of attack, or malware. Whereas a virus is designed to replicate itself, any software created for the purpose of destroying or unfairly accessing networks and data should be referred to as a type of malware.

Ransomware: Don't let all the other words ending in 'ware' confuse you; they are all just subcategories of malware. Currently, one of the most popular of these is 'ransomware,' which encrypts valuable data until a ransom is paid for its return.

Intrusion Protection System: There are several ways to safeguard your network from malware, but intrusion protection systems (IPSs) are quickly becoming one of the non-negotiables. IPSs sit inside of your company's firewall and look for suspicious and malicious activity that can be halted before it can deploy an exploit or take advantage of a known vulnerability.

Social Engineering: Not all types of malware rely solely on fancy computer programming. While the exact statistics are quite difficult to pin down, experts agree that the majority of attacks require some form of what is called 'social engineering' to be successful. Social engineering is the act of tricking people, rather than computers, into revealing sensitive or guarded information. Complicated software is totally unnecessary if you can just convince potential victims that you're a security professional who needs their password to secure their account.

Phishing: Despite often relying on face-to-face interactions, social engineering does occasionally employ more technical methods. Phishing is the act of creating an application or website that impersonates a trustworthy, and often well-known business in an attempt to elicit confidential information. Just because you received an email that says it's from the IRS doesn't mean it should be taken at face value -- always verify the source of any service requesting your sensitive data.

Anti-virus: Anti-virus software is often misunderstood as a way to comprehensively secure your computers and workstations. These applications are just one piece of the cybersecurity puzzle and can only scan the drives on which they are installed for signs of well known malware variants.

Zero-day attacks: Malware is most dangerous when it has been released but not yet discovered by cybersecurity experts. When a vulnerability is found within a piece of software, vendors will release an update to amend the gap in security. However, if cyber attackers release a piece of malware that has never been seen before, and if that malware exploits one of these holes before the vulnerability is addressed, it is called a zero-day attack.

Patch: When software developers discover a security vulnerability in their programming, they usually release a small file to update and 'patch' this gap. Patches are essential to keeping your network secure from the vultures lurking on the internet. By checking for and installing patches as often as possible, you keep your software protected from the latest advances in malware.

Redundant data: When anti-virus software, patches, and intrusion detection fail to keep your information secure, there's only one thing that will: quarantined off-site storage. Duplicating your data offline and storing it somewhere other than your business's workspace ensures that if there is a malware infection, you're equipped with backups.

We aren't just creating a glossary of cyber security terms; every day, we're writing a new chapter to the history of this ever-evolving industry. And no matter what you might think, we are available to impart that knowledge on anyone who comes knocking. **Get in touch with us today at info@palmtech.net or at (561)969-1616 and find out for yourself.**