PALMTECH
I.T. Solutions For Business

# THE LEGAL TECH TIMES

PalmTech Computer Solutions

December 2016

## Need To Upgrade Your Network? The Section 179 Deduction Can Save You $$, But You Must Act Before December 31st!

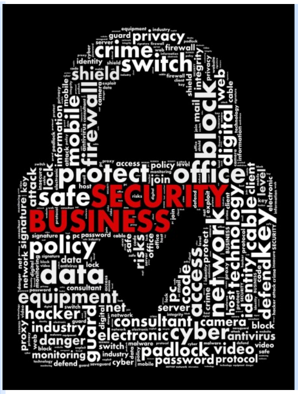
Visit
[www.PalmTech.net/section-179](www.PalmTech.net/section-179)
for details!

## December 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.



# $1.5M Cyber-Heist Typifies Growing Threat

Efficient Escrow of California was forced to close its doors and lay off its entire staff when cybercriminals nabbed $1.5 million from its bank account. The thieves gained access to the escrow company's bank data using a form of "Trojan horse" malware.

Once the hackers broke in, they wired $432,215 from the firm's bank to an account in Moscow. That was followed by two more transfers totaling $1.1 million, this time to banks in Heilongjiang Province in China, near the Russian border.

The company recovered the first transfer, but not the next two. They were shocked to discover that, unlike with consumer accounts, banks are under no obligation to recoup losses in a cybertheft against a commercial account. That meant a loss of $1.1 million, in a year when they expected to clear less than half that. Unable to replace the funds, they were shut down by state regulators just three days after reporting the loss.

Net result? The two brothers who owned the firm lost their nine-person staff and faced mounting attorneys' fees nearing the total amount of the funds recovered, with no immediate way to return their customers' money.

**Avoid Getting Blindsided**
While hacks against the big boys like Target, Home Depot and Sony get more than their share of public attention, cyber-attacks on small and medium-sized companies often go unreported, and rarely make national headlines.

Don't let this lull you into a false sense of security. The number of crippling attacks against everyday businesses is growing. Cybersecurity company Symantec reports, for example, that 52.4% of "phishing" attacks last December were against SMEs – with a massive spike in November. Here are just a few examples out of thousands that you'll probably never hear about:

- Green Ford Sales, a car dealership in Kansas, lost $23,000 when hackers broke into their network and swiped bank account info. They added nine fake employees to the company payroll in less than 24 hours and paid them a total of $63,000 before the company caught on. Only some of the transfers could be canceled in time.

continued on page 2

- Wright Hotels, a real estate development firm, had $1 million drained from their bank account after thieves gained access to a company e-mail account. Information gleaned from e-mails allowed the thieves to impersonate the owner and convince the bookkeeper to wire money to an account in China.

> “Require two people to sign off on every transaction.”

- Maine-based PATCO Construction lost $588,000 in a Trojan horse cyber-heist. They managed to reclaim some of it, but that was offset by interest on thousands of dollars in overdraft loans from their bank.

**Why You’re A Target – And How To Fight Back!**
Increasingly, cyberthieves view SMEs like yours and mine as easy “soft targets.” That’s because all too often we have:

1. Bank accounts with thousands of dollars.
2. A false sense of security about not being targeted.
3. Our customers’ credit card information, social security numbers and other vital data that hackers can easily sell on the black market.

If you don’t want your company to become yet another statistic in today’s cyberwar against smaller companies, and your business doesn’t currently have a “bullet-proof” security shield, **you MUST take action without delay – or put everything you’ve worked for at risk. The choice is yours.**

Here are three things you can do right away:

1. Remove software that you don’t need from any systems linked to your bank account.
2. Make sure everyone with a device in your network NEVER opens an attachment in an unexpected e-mail.
3. Require two people to sign off on every transaction.

**Let Us Help**
When it comes to defending your data, whether it’s bank account information, customer and employee records or proprietary intellectual property or processes, Do NOT take chances. Our experience and track record in keeping our clients’ data safe speaks for itself.

We are offering our ***Cyber Security Assessment at no cost through the end of December** to 10 companies in the South Florida area. Call us at **(561)969-1616** or e-mail us at info@PalmTech.net TODAY because we can only offer this valuable service to the first 10 companies that apply.

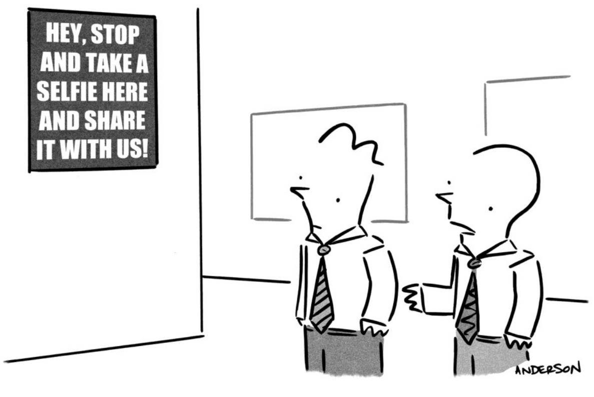
**Offer valid to qualified prospects with a minimum of 15 computers and at least 1 server.*

## 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.*

© MARK ANDERSON, WWW.ANDERTOONS.COM



“It’s cheaper than a security cam.”

## Shiny New Gadget Of The Month:

### Your Desk Is Killing You: Do This Instead

The evidence is piling up that sitting all day is bad for your health. Though not perfect, Varidesk offers a compelling solution.

On the plus side, The Varidesk sets up right out of the box – no assembly required. With its weight-balancing system, you don't need any hardware to fasten it to your desk. And it features an attractive, sturdy design. You can lean on it and your monitor won't go crashing to the floor. Springs and levers make it easy to raise or lower it to one of 11 preset levels.

The main flaw is that when you raise it, it also moves forward – a problem if you're in a tight space. All in all, though, it's worth looking at, especially if you have a wireless keyboard and mouse – and enough space in your office or cubicle to back up a bit.

# At The Office: Be The Adult In The Room

There's a reason people refer to the office as a "sandbox," because some folks refuse to act like adults. And, if the level of childish behavior rises to tantrum pitch and the culture becomes toxic, there's no chance for communication or growth. But the office is not a playground, and we're not children. So it's important that we enter into an "adult agreement" when we walk through the doors at work and begin our day.

When I work with companies looking to improve their business, one of the things we start with is our adult agreement. It informs the work we do for the entire day, and hopefully beyond.

Here are three agreements to make sure you're acting your age in the workplace:

**Don't shoot each other down.**

When a colleague brings an idea to the table – even if you disagree with it – don't shut them down just to be "right." If we want to be collaborative, we've got to consider that those around us have something valuable to offer. If you make it a habit to cut people off or discount what they're saying out of hand, you'll not only guarantee that they won't share their ideas with you again, but you'll likely miss out on insights that could help you and your company.

**Own up to mistakes and bring them to the table.**

Nobody is perfect – not you, not me, not Bill Gates or Mark Cuban or anyone you might admire in business. We all make mistakes, and the worst thing we can do is deny that they exist. Instead, own up to your mistakes and let everybody know what they are. We only grow and learn when we're vulnerable with each other. Admitting error is often considered a risk, but it's really an opportunity. Our mistakes let others understand who we are, what risks we're willing to take and what lessons we've had to learn. Share freely to engender trust and understanding among your teammates.

**Don't hide problems.**

Maybe you want to stay focused on the positive and don't want to highlight "problems." Wrong. You're not a negative person just because you bring problems to light or point out conflicts where they might exist. More likely, you're finally saying what everyone else is thinking and is afraid to say. Or you're bringing something up that's important for everyone to understand in order to improve and move forward. Put problems up for discussion and brainstorm solutions. Hiding problems only makes them grow.

As you seek to master these three steps, remember one more thing: adults don't crush each other just for acting like adults. We've got to support each other in our efforts to be truthful and vulnerable. A team is only as strong as its weakest link, so it's critical that we lift each other up.

When we act like adults – especially in the sandbox – we all win.

Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success and coaching them past the excuses. After all, as he tells his clients, 100% annual growth is only 2% growth every week. It's not easy. But possible. Andy learned how to build great organizations by building a great business, which he started in college then, grew into an Inc. 500 multi-million dollar national company that he successfully sold and exited. He founded Petra to pass on to other entrepreneurs, business owners and leaders the principles and practices he used to build his successful enterprise, which are rooted in the Rockefeller Habits methodology.

# Security Breaches: Tips For Prevention

As long as businesses host valuable data, cyber criminals will continue to bypass the security protocols meant to protect this data. The causes of security breaches range from device theft or loss, weak and stolen credentials, malware, and outdated systems that use ineffective security measures. And with these five tips, you can take the first step toward making sure a security breach never strikes at your precious business data.

## Limitation of lateral data transfers

Employees not being educated on data sharing and security is one of the biggest reasons for internal data breaches. It's a good idea to limit access to important data and information by restricting access privileges to only a small number of individuals. Also, you can decide to use network segmentation to cut unnecessary communication from your own network to others.

## Keeping your machines and devices updated

Internal breaches might also occur when employees work with unguarded or unprotected machines. They might unknowingly download malware, which normally wouldn't be a problem if machines were properly managed. Updating your operating systems, antivirus software, business software, and firewalls as often as possible will go a long way toward solidifying your defense systems.

## Use monitoring and machine learning to sniff out abnormalities

It's not all on your employees, however. Network administrators should employ monitoring software to prevent breaches by analyzing what is "normal" behavior and comparing that to what appears to be suspicious behavior. Cyber criminals often hide in networks to exploit them over a long period of time. Even if you miss them the first time, you should monitor suspicious activity so you can recognize impropriety and amend security policies before it goes any further.

## Creating strong security passwords and credentials

No matter how often we say it, there's always room for improvement when it comes to your passwords and login procedures. In addition to text-based credentials, you should require other methods whenever possible. Great for fortifying your network, fingerprints and smart cards, for example, are much harder for cyber criminals to fake. Regardless of which factors are used, they must be frequently updated to prevent breaches, accidental or otherwise.

## Security Insurance

In the end, no system is perfect. Zero-day attacks exploit unknown gaps in security, and human error, accidental or otherwise, can never be totally prevented. And for this reason, small businesses need to start embracing cyber insurance policies. These policies help cover the damages that might occur even under a top-of-the-line security infrastructure. Considerations for selecting a policy include legal fees, first and third-party coverage, and coverage for reputation rehabilitation.

The field of cyber security is overwhelming -- even for seasoned IT professionals. But not for us. We spend our days researching and experimenting to craft the best security solutions on the market. If you're interested in one of our cutting-edge cyber-security plans, call us today at **(561)969-1616** or email us at info@palmtech.net.