PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions JUNE 2016

Come See Us at the 2016 HFTP Florida Regional Conference

PalmTech Computer Solutions is sponsoring The 23rd Annual HFTP (Hospitality Financial and Technology Professionals) Florida Regional Conference held on July 20th - July 22nd, 2016 at the Wyndham Grand Jupiter at Harbourside Place.

Visit www.PalmTech.net/events for additional details.

HFTP Hospitality Financial and Technology Professionals

JUNE 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.

Shadow IT: Ignore At Your Own Risk

It's one of those little secrets that nobody wants to talk about…

The term "Shadow IT" refers to apps and devices used at work that operate outside your company's sanctioned policies and protocols.

Shadow IT takes many forms, like conversations on Facebook Messenger, Google Hangouts, Gmail or Skype. It can include software from Excel macros to cloud-based data storage apps such as Dropbox, Google Docs and Evernote. Or collaboration spaces like Slack, Asana and Wrike. And then there are devices: USB sticks, smartphones, tablets and laptops within your network that you have no control over.

Robert J. Moore, CEO of RJMetrics, relates how companies like Slack and Dropbox craft their pricing models to encourage rapid proliferation. One day, a few of his engineers were using Slack, then all the engineers, then the whole rest of the company was using it. He said, "We reached a point of no return and paying for it was pretty much our only option."

The hidden dangers of shadow IT

When users on your network adopt apps and devices outside your control, protocols aren't followed, systems aren't patched, devices get infected without people knowing it and data breaches happen… As a result, confidential information can be exposed, accounts taken over, websites defaced, goods and services stolen, and precious time and money lost.

Not only that, you end up with siloed information in unknown places, data compliance issues and missed opportunities for bulk pricing.

The obvious solution would be to crack down and forbid use of all but company-approved devices and apps. Unfortunately, that tends to slow things down, stifling

continued on page 2

productivity and innovation.

Bringing your shadow IT out into the light. Obviously, burying your head in the sand won't make the problem go away. Here's what you can do to not only take control of the situation, but actually use it to drive innovation and agility at your company.

> *"Take control of high-risk situations and keep an eye on the rest."*

Cut loose the "control" mentality. It's no longer feasible to simply ban certain apps. If you don't give employees the software they prefer, they may start using their own. They can easily access a vast and growing variety of apps, all without your help – or control.

Recognize the delicate balance between risk and performance. Evaluate risk on a case-by-case basis. Then take control of high-risk situations and keep an eye on the rest.

Foster open communication. Get employees involved in creating intuitive policies. You can turn them from your greatest risk to your greatest asset by levering their input and ownership of protective protocols. This helps everyone maintain security while keeping practical needs for performance in mind.

Develop a fully tested plan. Even if it's only 70% complete, a tested plan will be far more useful when the need inevitably arises than a 100% complete plan that's not fully tested. Most managers underestimate the confusion that occurs in the first few days following a breach.

Unfortunately, that confusion can create a defensive rather than constructive atmosphere centered on discovering how, when and where the breach occurred. A comprehensive incident response plan can go a long way toward achieving a speedy resolution, and keep an otherwise manageable event from turning into a full-blown business crisis.

Finding the right balance. Focusing only on security and asset protection can drag down business performance quickly. However, balancing risk with performance enables you to maximize your return from investments in detection and response. It also helps you become more adept at adjusting as the security landscape changes. By developing your organization's ability to recognize threats and respond effectively to incidents, you can actually take risks more confidently and drive business performance to a higher level.

PalmTech Computer Solutions can help you with this. Our proprietary **Security Assessment** helps you take the friction out of data protection. Contact us today at (561) 969-1616 or info@palmtech.net to take advantage of this offer (normally $497), FREE through the end of June, and put an end to Shadow IT in your organization finally and forever.

**Offer valid for qualified prospective businesses with 10 or more computers and a minimum of 1 server.*

Is Your Computer Data Truly Protected From Fire, Flood, Severe Storms or Even Theft?

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!

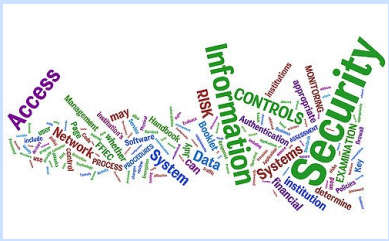
Popular Sites Forcing Reset of Passwords

Many sites are encouraging users to change their passwords as a result of the enormous amounts of data being sold on the dark web in recent weeks.

Facebook and Netflix have been report to be moving one step further by forcing their users to update their credentials. They are being cautious because many people use the same passwords on multiple accounts.

You may see more sites mirror this action in the upcoming weeks.

To protect yourself, make sure you change your passwords on your accounts and we recommend you make each password unique. If available, we recommend using two-factor authentication whenever you have the opportunity.



Who Gets the Blame When a Hack Occurs?

If a company finds itself on the receiving end of a successful hack, you would think the IT department or the information security officer would be carrying the blame. This isn't the case anymore as the higher ups are calling other, more powerful people responsible.

A recent survey found that of businesses who have suffered a security breach, the chief executive officers (CEOs) are being held accountable. When surveyed, directors listed the following in order of who needs to accept responsibility for failed cyber security: CEOs, CIO, entire C-suite, CISO, and board members.

Why are the CEOs first on the list? Maintaining up to date security is expensive and requires a great deal of time and resources. If CEOs haven't made cyber security a priority, then they would be to blame for the breach that a business is facing. In these instances, the security officer and IT department would not have had the financing necessary to protect the company to the best of their ability.

With the increasing number of cyber breaches happening to businesses large or small, executives have started to take security more seriously. Of the business surveyed, the majority reported that conversation around internet security is present at almost all board meetings. An overwhelming number also reported they feel their company is not as well protected and secured as it should be. The damage that comes in the wake of a security breach is a concern that more than 70% of the surveyed businesses shared.

While businesses are reporting the shift of focus for who's to blame when things go wrong, the security workers do not share their thinking. Across the board, the people employed in information security positions see themselves as taking the brunt of the blame if a cyber attack happened to them. Security is a team sport yet security experts feel they'll be the ones singled out from the rest.

The pressure on CEOs is causing many businesses to shift their resources to cyber security, making that department stronger and more efficient. The best case scenario shows CEOs, board members, and chief information security officers working together to best protect the company from cyber breaches and hackers. In the event of a security breach, it will be interesting to see who really ends up on the chopping block.

How Smart Office Buildings Are Dumbly Aiding Cyber Criminals

As buildings grow increasingly more intelligent with new technology, the corresponding risk of cybercrime to small- and medium-size U.S. businesses has grown.

Corporations have already been the victims of high-profile attacks, and the resulting media coverage has revealed vulnerabilities that all businesses share. Even a CCTV or air conditioning system can be breached—and with "smart" appliances, cyber criminals are already salivating at the possibilities.

It's not just simple hacks: ransomware (infecting a network and demanding a ransom to "fix" it), phishing (fraudulent emails that appear to be official) and more are huge threats to the credibility of a business and their ability to work.

It is smart appliances that worry experts the most: while a smart fridge can be run using an app, it is also highly accessible as compared to a traditional SAP system.

There are three steps businesses need to take to combat this growing hazard: 1) understand what smart technology does while it monitors your building and appliances, 2) work out if any valuable data is exposed and finally, and 3) find a security expert to safeguard that data.

The lost data need not be financial, either. Cyber-attacks may steal sensitive client or employee information. For medical and health businesses based in the United States, this could constitute a breach of HIPAA (Health Insurance Portability and Accountability Act)—resulting in costly legal action.

Ignoring these guidelines cost money: a 2015 IBM study revealed that one breach can cost the average company a cool $4m. With many nations adopting legislation that require enhanced data protection—at risk of fines and worse— these costs are only set to spiral.

As intelligent as the smart building may seem on the façade, the security risks cannot be overlooked.

Contact PalmTech Computer Solutions at info@palmtech.net through July 15th, 2016 for a **FREE Cybersecurity Assessment**. Our skilled security experts will come onsite, perform a step by step check to uncover your vulnerabilities , then we will draw up a plan to secure those "holes" to minimize risks to your data and network. Act now to ensure your business is protected. Cybercriminals may well ransack your business next.

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/

"Come on you guys. If you're gonna snicker every time I say 'dump file' we're gonna be here all day."