szymanski
CONSULTING

August 2013

Cathy's Message

WOW, July went by quickly. Hope it was a great month for you.

David and I did some traveling recently. We had a Kiwanis International Convention in Vancouver. Vancouver was beautiful and the people were simply amazing.

At the convention I was humbled by receiving Distinguished Kiwanis Governor for last year. Only seven districts in the America's received this award last year. It is the first time Pennsylvania has received it in several years, since 2006

We also traveled to Nashville for a very enthusiastic high energy conference that truly was remarkable. It does not matter how long we have been in business, or how old we are, we have to keep educating ourselves and our clients.

We hope you know how much we appreciate all of you and if there is something you would like to see us selling, please reach out and let us know.

Thank you for a great July!

Take care and have the best month ever!

Cathy & David

Five low cost security tips

A common misconception among many business owners and managers is that managing the security of their systems and computers is a time-consuming and costly endeavor. While it certainly can be expensive, how much you spend really depends on the type of security you want and need. In fact, there are security steps you can take that won't cost you much in the way of time or money. Here are five low-cost things you can do to ensure that your business is secure.

1. Keep important systems off site Many small to medium businesses keep their serv ers on site. While this is convenient as your systems are right there and easily accessible, this could also create a security issue. One way to minimize this is to work with us and we can host your systems or servers off site or in the cloud. While this involves some cost, working with us could save you profits and productivity in the long run, we will ensure that your systems are secure and working properly.

continued on page 2...

I need your help on this...

Dear Friend,

I have a small favor to ask that in the end will benefit you. But first, let me explain what's led up to this…

Over the last year, we've seen a dramatic increase in the number of clients who are inquiring about how to access their desktop files, email, etc. on a mobile device - be it an **iPad, smartphone, laptop, tablet**, etc. We've also seen an increase in the number of clients who allow employees to bring their own devices to work and/or access the company network from home using their personal computer or phone. If you've been following along in the last 2 issues of this newsletter, you've probably noticed.

Naturally, this raises a NUMBER of questions and concerns over security:

What's the best way to allow remote access to company data?

What are the best policies for privacy and cloud computing?

How can we ensure our compliance with data breech laws and regulatory controls?

That's why we've decided to hold a series of educational seminars (or webinars) on this topic in the coming months to answer important questions and to guide clients to use safe, best practices when introducing mobile devices onto their network.

However, I'm struggling to narrow down the topic and the questions we should address during these sessions since mobile and cloud computing are such big topics.

So instead of just guessing, I was hoping you could do me a favor by answering the following 2 questions:

"What is the single most important question you would like us to address on the topic of mobile and cloud computing?" Second...

"What's the single biggest CONCERN you have about cloud computing and employees remotely accessing your network with mobile devices?"

__PLEASE__ take a moment to send me an email at cathy@szy.com and give me some direction in this, I would be grateful. Many thanks! **Cathy**

Bizarre and Unique Holiday's in August

- Admit You're Happy Month
- Family Fun Month
- National Catfish Month
- National Eye Exam Month
- National Golf Month
- Peach Month
- Romance Awareness Month
- Water Quality Month

* National Picnic Month1870s. Students started throwing them in the 1940s.

Tips & Tricks

As you work with the mouse in Word, you have no doubt noticed small yellow boxes that pop up near the mouse pointer and indicate information about whatever you are pointing at. In Word, these are called ScreenTips. By default, they are turned on, meaning they are displayed. If you find them distracting, you can turn them off by following these steps:

- Choose Options from the Tools menu. Word displays the Options dialog box.
- Make sure the View tab is selected.
- Make sure the ScreenTips check box is cleared.
- Click on OK.

Videos

We hope you are enjoying our weekly videos. If you have a specific topic you would like to see us cover please let us know.

If you would like us to add someone onto the list we will certainly take care of that.

We feel the more education we can get out to you, the better.

Five low cost security tips

Continued from page 1…

2. Communication is key Many companies take steps to ensure that their systems are adequately protected. The thing is, many security breaches come from within the company. If your employees keep passwords written on pieces of paper that they leave lying around their desks, this is a security issue. It is a good idea to agree with employees where to keep important information and ensure they follow these rules. Beyond that, if you implement security changes or new systems e.g., new virus scanning software, it is important that you talk to your staff to ensure they know how the system works and how they can use it. You would be surprised at how much effective communication can help to minimize security issues, and best of all? It's free!

3. Educate your staff One of the more common security issues comes from spam and malware found in emails. It is a good idea to educate your staff on how to spot these different types of emails and other malicious websites, as well as how to avoid them.
It is worthwhile ensuring that your employees know their roles when it comes to security too. If you have a secretary who you believe is responsible for ensuring the office is locked at the end of the night, take steps to ensure that this person understands their responsibilities. The same goes for computers your staff use: If they are responsible for conducting security scans let them know this. While this may take some time, the cost is low to free.

4. Keep track of your keys To ensure the security of your IT systems and your physical office, you should keep control of your keys. That is, both the physical keys and those associated with your software (the codes you enter to verify software and unlock full versions).
Keep track of which staff members have a key to the office and if possible number them. The goal here is to know where your keys are at any given time, and if a staff member changes employers make sure you ask for them back.
Many software keys or licenses are single use only. If you invest in software and an employees steals this along with the key, you will likely have to purchase the software again. A good tip is to keep software keys secure and separate from the software itself. The best part about this step is that the cost of doing this is minimal.

5. Keep your software updated Hackers can be a lazy bunch. They will often target those with out of date software, because it's usually easier to hack. To reduce the chance of being hacked, you should take steps to ensure that your software is up-to-date. This includes your virus and malware scanners, as well as browsers and even software you don't use.
Get your staff or Szymanski Consulting, to perform a 'software audit' on their computers on a regular basis. This means going through their computer and properly uninstalling software that they don't use, while also taking time to ensure their system is completely updated. This step is easy to implement and will cost you next to nothing.

If you are looking to make your systems more secure, please contact us today. We may have a solution that will work for your business. cathy@szy.com 814-455-6069 x300

Cathy's useless trivia:

Did you know that 40% of McDonald's profits are from the sales of Happy Meals? Did you know that Walt Disney was afraid of mice? Did you know that Casey Kasem is the voice of Shaggy in Scobby-Doo. Here's a practical one for you, rubber bands last longer when refrigerated. Maine is the only state whose name is just one syllable. Do you have any useless trivia to share, send it to me and we will post it.

Do your employees bring their own devices to work?

The evolution of personal mobile devices and the rise of how necessary they are to business success these days are forcing many small business owners to make a choice - **"Bring Your Own Device" (BYOD)** vs. **"Corporate Owned, Personally Enabled" (COPE).**

The Typical Solution - BYOD. According to the CDW 2012 Small Business Mobility Report, **89% of small-business employees use their personal mobile devices for work**. But the headache involved here is how do you support and secure all of these devices? The scary thing is that most small businesses don't even try! The CDW survey found that only 1 in 5 small businesses have deployed (or plan to deploy) any systems for managing and securing employees' personal devices.

The Alternative - Is COPE Any Better? A minority of small businesses has implemented a Corporate Owned, Personally Enabled ("COPE") policy instead. They buy their employees' mobile devices, secure them, and then let employees load additional personal applications that they want or need. And the employers control what types of apps can be added too. And the "personally enabled" aspect of COPE allows employees to choose the company-approved device they prefer while permitting them to use it both personally and professionally. COPE is certainly more controlled and secure, but for a business with a limited budget, buying devices for every employee can add up pretty quick. If you go the COPE route and are large enough to buy in volume, you can likely negotiate substantial discounts.

Security Concerns With BYOD. If you have client information that must be kept secure or other industry specific regulations regarding the security of client data, then COPE is likely your best approach. It takes out any gray area of whose data is whose. Plus there is a certain comfort level in being able to recover or confiscate any device for any reason at any time to protect your company without any worries of device ownership.

Five benefits of offsite backups

One common threat to businesses is disaster. One can strike at any time and can vary in severity. Regardless of whether a company is facing a major catastrophe or something as simple as spilling water on a keyboard, it is a good idea to take steps to prepare for different potential disaster scenarios. A way to prepare for disaster is to back up your data using an offsite backup solution.

Here are five benefits and a definition of offsite backup.

Offsite backup defined The definition of offsite backup can be a bit difficult to nail down, as when many IT providers talk about this idea they are usually referring to one of a number of different kinds of backup. The key idea revolving around offsite backup is that your company's data and backups are sent out of your physical location(s). In other words, your backups are not stored in your office or building.

Offsite backup is usually done in one of two ways:

Physical transport - This can range from something as simple as copying important files onto a removable hard drive and storing this in another location, to backing up entire systems on tape and storing them off site.

Remote backup - This is a more modern approach to data backup, whereby your data and files are stored on servers located off site. This form of backup is commonly referred to as 'cloud backup'.

For the purpose of this article, we will focus on remote backup as this is the main solution companies are enquiring about.

Benefits of remote backup

1. It's more reliable: The major benefit of remote backup is that it can be automated. Your files are updated on a daily basis, or you can set the time for the update. Because these solutions work over the Internet, you will be able to recover files quickly. Beyond that, the servers that offer this solution are often located in numerous locations, which ensures that your backups are always available, even if a server crashes.

2. It reduces workload: Traditional backup solutions require a person, whether you or an IT professional, to manually back up or copy files. This can take a long time, and will take you away from your normal job. Many remote backup solutions can be initiated at the click of a mouse after setup, or can be scheduled for when you aren't in the office.

3. It's easy to set up: Backup solutions are managed by an IT partner who can work with you to set up which files and data to back up. Other solutions can be set up with a few clicks and even automated, so you can rest assured that your data is backed up and up-to-date.

4. It's secure: Most backup providers store their servers in secure locations, meaning that your data is physically secure. To ensure that backup data is transmitted securely, most solutions use advanced encryption tools to keep data secure.

5. It will save money: If you have numerous computers with large amounts of data that you back up regularly, you know that physical storage solutions can be costly. The majority of remote backup solutions are billed on a monthly-basis and support a near unlimited amount of backup space. If your company operates in an industry where backups are mandatory, or you have a large amount of files to back up, these options will save you money. If you are interested in learning more about how offsite, remote backup can help ensure that your business is ready for disaster recovery, please contact us today 814-455-6069 x300 or cathy@szy.com

A new way hackers are gaining access

Do you have Java turned on in your web browser? If your answer is "Yes" or "I'm not sure" then it's time to take action to find out. Why? The biggest threat to your computer systems in 2013 (and beyond) is no longer Microsoft Windows - it is Oracle Java.

After 20+ years as the poster child for insecure software, Microsoft's newest operating systems (Windows 7 and 8) have gotten their act together. Cybercriminals like to get the greatest bang for their buck and therefore they're attacking the Java platform because of its huge market share and because it's an easier platform to hack than the Microsoft operating system. Java is now installed in over 1.1 billion desktops and 3 billion mobile phones. That's a big target that is very attractive to hackers. Hackers also love that Java is multi- platform, which means it's capable of corrupting PCs running Windows, Mac OS X or Linux. And since many Mac users don't have anti-virus, hackers were able to infect over 600,000 Macs with serious malware via the Java software installed on their machines.

Right now, cybercriminals are aware and exploiting any security flaws in Java that could lead to infections on your computer. There are even automated kits now available to capitalize on any security hole found within days, if not hours of them becoming known. It's not unusual to see hackers use Java as a first attack to weaken the defenses before serving up an Operating System specific attack. Even the Department of Homeland Security suggested that "To defend against future Java vulnerabilities, their users should consider disabling Java in web browsers."

Here are 3 steps you can take today to minimize your risk:

- Disable or uninstall Java wherever you can. If you don't need it, remove it.
- Where Java is necessary, use a separate web browser only used for Java based websites and be sure to patch Java regularly.
- Have your staff report the first signs of slowness, Possible infections and web browser popups to your IT guy as soon as they happen.

"Dear Andy: How have you been? Your mother and I are fine. We miss you. Please sign off your computer and come downstairs for something to eat. Love, Dad."

Taking Referrals

Do you have anyone you would like to refer to us! We have a referral program that we would love to share with you. Please email Cathy today to find out more information.

szymanski
CONSULTING

BBB. ACCREDITED BUSINESS

Manufacturer & Business ASSOCIATION www.mbausa.org

technology council of Northwest PA

ERIE REGIONAL CHAMBER AND GROWTH PARTNERSHIP

Business Partner IBM

lenovo

xerox

CISCO PARTNER Registered

Microsoft Small Business Specialist

Microsoft Partner
Gold Desktop
Silver Midmarket Solution Provider

Varnex™

ascii the ascii group, inc.

CompTIA

Kroll Ontrack

Szymanski Consulting, Inc.
8127 Nathan Circle
Erie, PA 16509
814-455-6069
www.szy.com

szymanski
CONSULTING