



January 2014

Cathy's Message

Happy New Year! This year is going to be an amazing year filled with inspiring success stories of our customers. David and I have made business goals around our customer's businesses and philosophy's. We are excited for what the New Year will bring for all of us. We are hoping you will continue asking questions and giving us ideas for the newsletters. We also hope you send us videos. If you would like to receive our videos, email me to let me know. Most importantly we want to grow with you. Your business is very important to us and we want to be there for you. We also hope you will send referrals our way. We have incentives for referrals and would love to talk to you about them. We

are always here for you. We look forward to another EPIC year working with you and your staff and sincerely hope that 2014 is your absolute best year ever. Cathy & David.

truly value you and please know that we

Did You Know

- A man patented something eerily similar to an iPod in 1979!
- The power source for NASA's Curiosity rover barely outputs enough energy to power a ceiling fan!
- Google has bought an average of one company per week since 2010!
- Smoking near Apple computers voids the warranty.
- The Recording Industry Association of America tried to outlaw MP3 players in 1998!
- MIT has built a robot that can assemble IKEA furniture on its own!
- There is a \$300,000 watch that doesn't tell time!
- The default Windows XP desktop is a real picture of a real location with no digital enhancements. The background is called "Bliss" – a green meadow with a blue sky above it.

Plan The Migration Now To Protect Your Business

Microsoft is ending support for Windows XP and Office 2003 on April 8, 2014. If your organization has not started the migration to a modern desktop, please start now, the **COUNTDOWN IS ON.**

To ensure you remain on supported versions of Windows and Office, you need to begin your planning and application testing **immediately** to ensure you deploy before end of support.

What does end of support meant to



After April 8, 2014 there will be no new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates.

Running Windows XP and Office 2003 when support ends may expose your company to potential risks. Therefore, any computer or server with these software programs installed will be completely exposed to serious hacker attacks aimed at taking control for your network, stealing data, crashing your system, and inflicting a host of other business-crippling problems you do not want to have to deal with.

Don't wait until the last minute to plan for an XP-free business existence. We fully expect to be extremely busy now through April 8.

Schedule your Microsoft XP Risk Assessment and Migration Planning Consultation today by calling our office at 814-455-6069 x300 and ask for Cathy



New Year's Resolutions To Make in 2014

Besides resolving to spend more time with family and friends, getting fit and getting organized, have you made any New Year's resolutions for your business?

Looking at your current computer network and reviewing your past year's network support and services, are you saying to yourself, "I'm not going to let this happen again in 2014!" Do any of your New Year's resolutions include dealing with continually pesky computer network issues?

Do Your Resolutions Look Anything Like This?

RESOLVED, double pinkie shake, I WILL get my critical company data automatically backed up offsite daily. Whether through fire, natural disaster, tape failure or just human error, I might lose all of my company data, which will cost me plenty.

RESOLVED, I will take a serious look at cloud computing and all of the business benefits and potential savings the cloud offers for my business.

RESOLVED, I will not tolerate subpar security policies or procedures for my company that put it in a high-risk category for being subject to cyber attacks that could cripple or completely wipe out my business.

FREE Technology Business Review Gets You On The Road To Keeping Your Resolutions And Eliminating Your Day-To-Day Computer Headaches.

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.

Five Top Health Care Stories Of 2013

As 2013 came to a close, we looked back at the health-care information technology (IT) stories that most captivated the industry. Some were bad (because bad news makes headlines), but some were also good. Here are five topics we found most intriquing.

The Internal Revenue Service (IRS) faced a class-action lawsuit over the theft of 60 million medical records. Allegations arose that the IRS improperly accessed the health records of 10 million Americans, including those of California state judges.

Unhappy electronic medical record (EMR) users began switching systems. With numerous EMRs falling short of providers' expectations, Black Book Rankings reported that 2013 may have been the "year of the great EHR vendor switch."

The Department of Health and Human Services (HHS) made sweeping changes to HIPAA. An eagerly awaited set of regulations in the health-care arena arrived on January 17 when HHS issued modifications to the HIPAA privacy, security, enforcement and breach notification rules.

More physicians began sharing their written notes with patients. It's a growing trend, and not such a bad idea, says one industry attorney and consultant.

Google Glass arrived. It was the most anticipated new gadget since the smartphone, and potentially transformative - but it came with controversy, and how it will be used in health care is yet to be seen. That being said, there could be some interesting uses especially in surgery or even diagnosing patients - wouldn't it be cool to be able to call up a record that you can read without paper!

If you are looking to learn more about how these stories affect you, contact us today to see how we can help.

Shiny New Gadget

The iPhone/iPad Pocket Projector

Now you can share the latest YouTube sensation, share that adorable video of kitty doing her tricks or watch a movie on the big screen, all from your phone. With the iPhone/iPad Pocket Projector, your iPhone's screen can project an image reaching up to 85 inches diagonally and from as far as 10 feet away. It's simple, easy to use and super quick to set up this mini-device.

The projector weighs less than 5 oz. and is smaller than a smartphone. The iPhone/iPad Pocket Projector can turn your ceiling, tent, blank wall or even the side of your house into a movie theater. The projector's 640 x 480 pixel resolution ensures a nice picture, and a man-



ual focus wheel enables you to "dial up" sharpness and clarity. (The sound still comes from your iPhone speaker, so for the best quality, you may want to invest in some new speakers to stream the audio.)

A free app enables you to magnify or rotate images and project everything from videos to a four-hour search for the perfect shoes. The internal battery provides two hours of projection and recharges via USB with the included cable. This device is compatible with most iPhones/iPads, except the iPhone 5, the new iPad with Retina Display and the iPad Mini. Get one today at www.amazon.com.

Two Million Passwords Stolen! Were You Hacked?

On December 3, 2013, security company Trustwave discovered over two million stolen user passwords for popular online services like Facebook, LinkedIn, Google, Twitter, Yahoo, and 93,000 other websites. There's a high probability that you use one of the services affected by the hack. Is your personal information compromised?

These passwords were stolen from users' computers and stored on a server in the Netherlands. The collection of these passwords was the work of a botnet called "Pony." The botnet primarily collected data through email phishing scams, and it was discovered that data in this password cache belonged to users from 102 different countries. The collection campaign appears to have been accumulating login credentials since October 21, and it's likely still active.

Trustwave immediately notified every company affected by the hack. The hacked companies reset the passwords of the affected accounts and notified the affected users of the breach. The website with the most passwords stolen was Facebook with 318,000, however the hacked company that possesses the biggest risk to businesses is ADP, which is a popular payroll management app. ADP commented about the hack of 8,000 of its passwords and stated that, "To our knowledge, none of ADP's clients has been adversely affected by the compromised credentials."

Have You Been Hacked?

If you haven't been notified yet of the hack, then your password hasn't been compromised. The big takeaway from this news story is the importance of password security. Poor password management can put your business at serious risk. Here are a few tips that will help keep your accounts safe from hacking: Use Complex Passwords: Using complex and impossible to guess passwords for all of your accounts is one of the most fundamental variable of protecting your sensitive information. **Update Your Software:** The value of updating your software (especially your antivirus software) is that the updates include security patches that will protect you from known viruses. Running outdated software will leave your system vulnerable. Be Mindful of Phishing Scams: Your email inbox gets hit with scams every day, and there are malicious sites on every corner of the Internet that could infect your computer with malware. You need to educate your staff on what to look for when using the

Cycle Out Your Passwords: You don't have to wait until you receive a notification that you've been hacked to change your password. It's best practice to cycle out your old passwords for new ones every few months.

Use Multi-Factor Authentication: Many services like Facebook and Google offer users multi-factor authentication. This adds an extra step to the login process that increases security. The most common way this works is with a two-factor authentication procedure where you first enter your password, and then you will receive a text containing a unique code that gives you access to your account.

One of the best steps you can take to protect your business from identity theft is to have a reliable network security solution. We can provide your network with a bullet-proof firewall, along with content filtering capabilities to protect your system from malicious websites. To batten down the hatches on your network and keep your passwords safe from hackers, give us a call today at

814-455-6069 x 300 or email cathy@szy.com

The leaders who work most effectively, it seems to me, never say 'I.' And that's not because, they have trained themselves not to say 'I.' They don't think 'I.' They think 'we.' They think 'team.' They understand their job to be to make the team function. "Peter Drucker 1909-2005"

Public Wi-Fi Security Issues

There is a trend among many businesses of connecting to the office from outside, or doing work remotely. In order to do so, most users require an Internet connection, often using public Wi-Fi connections. The issue with many public Wi-Fi connections is that they may not be as secure as you think, and could lead to increased security threats and even loss of data.

If you or your employees work outside of the office, and rely on, or frequently connect to public Wi-Fi connections, there are three security dangers you should be aware of.

1. Fake networks

The number of businesses offering free Wi-Fi to customers, especially coffee shops and restaurants, is growing. Some hackers have actually taken to setting up networks with names that are the same as a location or business in hopes that people will connect to it, believing it is an open network.

The issue is that they may have attached data monitors that collect data - including passwords and other private information going into and out of the network. Some have even gone so far as to set up a portal site that one must navigate to in order to log in and use the service - similar to what you see when you use most public Wi-Fi connections. Only these sites are loaded with malware which can be installed onto your system once you log in.

In order to avoid this, it is a good idea to look at the name of the network you are actually connecting to and check whether there is more than one with a similar name, or if there are any spelling mistakes. If you are unsure, check the name of the network at the business which is providing this connection.

2. Shared files or folders

Both major operating systems - OS X and Windows - have files and folders that automatically share any folders and files put into them with other users on the same network. Some business users put important files in these folders while at the office in order to allow colleagues access to them.

The problem with this is when you connect to a public Wi-Fi connection. Other people on that network may also be able to see those files. If you didn't take the important files out of the folder, they could potentially steal the data contained within. Hackers know this, and may sit on the networks looking for other computers with shared files.

In order to avoid this, ensure that you aren't sharing files stored in public folders on your computer. Try using other ways to share documents like a cloud storage provider.

3. The man-in-the-middle

A man-in-the-middle attack is a form of hacking where the hacker uses technology to actively listen to or capture data being transmitted over a network. What this means is that if there is someone capturing data, they could theoretically gain access to anything that gets sent outside of the network. This could include private files, passwords and more.

If you or an employee connects to the office remotely while connected to a public network, one way to minimize the chances of data being intercepted is by using a VPN. These connections set up a direct link between the computer and the home network, and make it difficult for those who aren't part of that network to connect to and view data that is transmitted over this connection.

It is a good idea to avoid entering passwords or other important information like bank account and ID numbers while connected to public networks.

Contact us today to see how we can keep your data secure while out of the office.

Business Intelligence Trends For 2014

In 2013, Business Intelligence - transforming data into useful information that can be used by managers to make decisions - has become a popular process used by businesses to make better decisions. You will continue to hear about it in 2014. Here is an overview of the potential Business Intelligence (BI) trends we could see emerging and growing in 2014.

1. BI is more accessible

Historically, to get the most out of Business Intelligence you need to be experienced or to employ a data scientist. Over the past couple of years BI methodologies have become easier to execute. Throughout 2014 it is highly likely that we will see most business users continue to gain skills in this area and consequently carrying out business analysis and BI activities.

This means we should see an increase in the number of programs that are user-friendly, while still providing the powerful tools that experts have been using.

2. Bl and Big Data solutions forecast clouds

Cloud-based solutions have helped allow small to medium businesses to access tools that were previously only used by enterprises. Many BI solutions are starting to incorporate cloud-based versions and this trend will continue in 2014.

These solutions will put important data in the hands of individual businesses, while also providing them with the ability to store and analyze their data with ease, as long as they have an Internet connection. Many of these solutions also allow for increased collaboration and some even have mobile apps which could help make adoption easier.

3. Predictive analytics are more accessible

Predictive analytics is the process of looking at existing data for trends and important information that you can use to help make predictions and decisions. This type of analysis has largely been the domain of experts and large companies, but in 2014 this process should become increasingly available to small businesses.

4. Social data is even more important

The majority of customers are active on social media. This has led to a huge source of potential information that businesses can benefit from. From Likes to Shares, Comments, etc., companies will begin to pay closer attention to this data. It can help businesses gain insight into brand awareness, how relevant they are to customers, and even gain important information they can use to conduct competitive analysis.

5. Storytelling from existing data

One of the main objectives of analyzing your data is so that you can tell a story with it. If you have no narrative arc attached to your data, it is highly likely that the message you want to get across won't sink in.

By visualizing your data in a way so that it tells a story you will be better able to gain a concise meaning from an overwhelming amount of data

If you are looking to learn more about BI and how it can help your business, please contact us today.

O MARK ANDRESON, WWW.ANDRETOONS.COM



"Oh, that? We don't know what that is. The plan is to just ignore it and hope it goes away."





















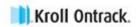












Szymanski Consulting, Inc. 8127 Nathan Circle Erie, PA 16509 814-455-6069 www.szy.com



