Business System Solutions

The BSS Advisor

January 2017

3 "Must-Do" IT Resolutions For 2017

"Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today." That's what *The Evolution of Ransomware*, a study by Mountain View, California-based cybersecurity firm Symantec, reported recently.

If you have any illusions that your company is safe from cyber-attack in 2017, consider just a few findings stated in a recent report by the Herjavec Group, a global information security firm:

- Every second, 12 people online become a victim of cybercrime, totalling more than 1 million victims around the world every day.
- Nearly half of all cyber-attacks globally last year were committed against small businesses.
- Ransomware attacks rose more than an astonishing 300% in 2016.
- The world's cyber-attack surface will grow an order of magnitude larger between now and 2021.
- The US has declared a national emergency to deal with the cyberthreat.
- There is no effective law enforcement for financial cybercrime today.

Clearly, your company's information and financial well-being are at greater risk than ever in 2017. And you cannot count on the federal or state government or local police to protect your interests. That's why I STRONGLY SUGGEST that you implement the following resolutions starting TODAY.

Resolution #1: Tune up your backup and recovery system. The #1 antidote to a ransomware attack is an up-to-date backup copy of all your data and software. Yet managing backups takes more than just storing a daily copy of your data. For one thing, if your business is at all typical, the amount of data you store grows by 35% or more PER YEAR. If your data management budget doesn't expand likewise, expect trouble.

Resolution #2: Harness the power of the cloud—but watch your back. Huge productivity gains and reduced costs can be achieved by making full use of the cloud. Yet it's a double-edged sword. Any oversight in security practices can lead to a breach. Here are two things you can do to harness the cloud safely:

-Determine which data matters. Some data sets are more crucial to your business than others. Prioritize what must be protected. Trying to protect everything can take focus and resources away from protecting data such as bank account information, customer data and information that must be handled with compliance and regulatory requirements in mind.

-Select cloud providers carefully. Cloud vendors know that data security is vital to your business and promote that fact. Yet not all cloud vendors are the same. You can't control what happens to your data once it's in the cloud, but you can control who's managing it for you.

Resolution #3: Set and enforce a strict Mobile Device Policy. As BYOD becomes the norm, mobile devices open gaping holes in your network's defenses. Don't miss any

(continued on next page)

Lafayette Office:
1211 Cumberland Ave.
West Lafayette, IN 47906
(765) 742-3440

Kokomo Office:
3138 S Lafountain St.
Kokomo, IN 46902
(765) 507-9583

www.bssconsulting.com

BSS is your IT Partner providing **Total Care** support for all your technology needs with exceptional **Customer Service** and the best IT Solutions to make ***your business*** more productive and profitable!

A publication of Business System Solutions, Inc. | Managing Technology For Small Businesses Since 1995

IT Security Tip #12: DANGERS of Dropbox and other file sync apps

If you're using Dropbox, OneDrive, Google Drive or any other consumer-grade file sync and sharing cloud applications, listen up! These applications pose a huge threat to your company because company data can be spread far and wide without central oversight of what information is being shared with whom. Furthermore, over 7 MILLION Dropbox accounts have been hacked, giving cybercriminals a path into the company's network.

This is even MORE important if your company has access to and/or stores financial, medical or other sensitive data. Using file-sharing applications like these are a clear and direct violation of data breach and compliance laws. Bottom line, DON'T USE THEM FOR COMPANY DATA and use only company-approved, business-grade file-sharing applications.

of these three crucial steps:

-Require that users agree with acceptable-use terms before connecting to your network. Be sure to include terms like required use of hard-to-crack passwords, conditions under which company data may be "wiped" and auto-locking after periods of inactivity.

-Install a Mobile Device Management System on all connected devices. A good system creates a virtual wall between personal and company data. It lets you impose security measures, and it protects user privacy by limiting company access to work data only.

-Establish a strong protocol for when a connected device is lost or stolen. Make sure features that allow device owners to locate, lock or wipe (destroy) all data on the phone are preset in advance. That way, the user can be instructed to follow your protocol when their phone is lost or stolen.

Our Free Network And Security Audit Resolves Your Biggest Data Security Problems and Makes Your Systems Run Like A Fancy Swiss Watch

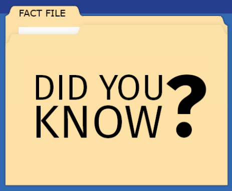
Ever asked yourself why some business owners and CEOs seem so blithely unconcerned about data protection? Don't let their ignorance lull you into a false sense of security. If you've read this far, you are smart enough to be concerned.

Call us right now at (765) 742-3440 and we'll send one of our technicians over for a FREE Network and Security Audit. It's your best first step to a safe and prosperous 2017.

Our Clients Say It Best

"Business System Solutions, Inc. (BSS) has been our IT company for over 15 years. BSS is a superior IT company in that their services consist of the ability to remote in to your computer and fix any problems that may arise during the day. BSS will notify you when something wrong occurs. BSS provides us with monthly reports. BSS have saved our company on many occasions throughout the 15 years of doing business with them. We appreciate the great service and the wonderful staff that provide us with their services throughout each and every year."

-Patti Kidwell, Robison & Bergum

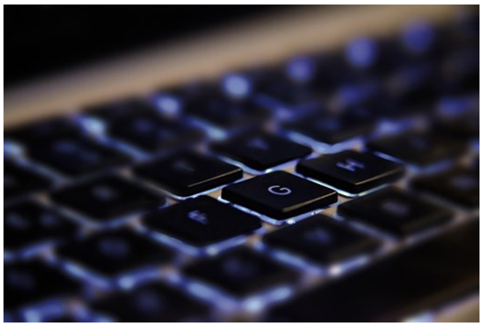


- Over 169 million personal records were exposed in 2015, stemming from 781 publicized breaches across the financial, business, education, government and healthcare sectors.
- The median number of days that attackers stay dormant within a network before detection is over 200.
- As much as 70 percent of cyberattacks use a combination of phishing and hacking techniques and involve a secondary victim.
- 30% of phishing emails are opened. And about 12% of targets go on to click the link or attachment.
- 68% of funds lost as a result of a cyber attack were declared unrecoverable.
- The cyber insurance market—mainly a U.S. market—has grown from $1 billion to $2.5 billion over the past two years, and it is expected to grow dramatically and expand globally over the next five years.

© Mike Baldwin/Cornered

"Elizabeth, we picked up a virus. Fortunately, we had everything backed up on memory sticks."

Did The Internet Crash Because Of...You?



In today's world we rely more and more on technology. Many businesses close when their computers are not working, and would close permanently if they lost their data. As our vendors change from selling software, to just selling the use of their software over the internet, we have also become extremely reliant on the internet for our business.

The internet is critical for our business activities like email, purchasing, sales, and our line of business software. But it is also the biggest source of the disruptions to our technology.

So how is the internet the source, and how do the hackers get in? As the hackers are traveling the highway of the internet they turn in every driveway to see if they can get into your office. At the gate or locked door of the firewall they are stopped most of the time. Even the basic routers from cable and other internet providers will give you basic protection from the simple outside attacks.

The goal of these hackers is to get a small program installed on your computer where they can send it commands. Those commands can do things like capture keystrokes (passwords), send out spam to the world, throw a lot of ads up on your screen, encrypt all your data, or even cause your computer to send out bogus traffic to take down a website like what happened on October 21st, 2016.

How the heck do they get in to put that malware or virus on your system? Most of the time they manipulate the user to open an attachment that is the source of the hacker's program, or to go to a website, that behind the scenes takes advantage of a Windows flaw and installs the bad program.

Since the initial firewall blocks the hacker from getting in, now you have unintentionally invited them in by clicking on the link, or opening the attachments. Now your PC, and potentially all PCs in your office, are now part of the hacker's arsenal to collect information, disrupt your business, or attack another entity on the internet.

Are you part of the problem? Is your system protected? What we do for our business and our clients is provide several 'layers' of protection. The absolute most important is a good backup that keeps hourly backups and is monitored daily to assure it is always working.

The other layers help keep you from being part of the problem as well as protect you. Some of these are a firewall that is a UTM (Unified Threat Management), good passwords, keeping Windows and software updated, antivirus and antimalware software that is updated and working, and good spam filter for your email. But ultimately, with all the technology, to avoid being part of the problem and protect your valuable information you must continually educate users what is safe and where to be vigilant when opening attachments and clicking on web links!

Here's an easy way to start 2017 with a clean e-mail in-box.

Ever wonder how in the world you ended up on so many e-mail lists? They just pile up until you can't even keep up with unsubscribing from the new ones. Unroll.me lets you manage your subscriptions by unsubscribing and bundling the ones you want to keep into a single daily "rollup." It makes unsubscribing easy and painless. It simply lists all your subscriptions for you. You just click an X next to the ones you want to unsubscribe from and Unroll.me takes care of the rest. It's a great way to organize your in-box while keeping all the subscriptions you love. *Lifewire.com, 10.17.16*

Progress doesn't have to grind to a halt during an Internet outage.

First, realize how a loss of Internet access messes with people's heads. When you can't connect with people online, your primal brain feels isolated because it sees inclusion as key to survival. Then there's that little endorphin rush you start missing when you can't check a task as complete. Add to all that a fear of missing out (FOMO) when you lose touch with friends on Twitter, Facebook or e-mail, and you have a formula for widespread panic among the troops. Instead, keep your cool and carry on with these four activities: 1) Call a meeting, or do training. 2) Complete your "later" list. 3) Compose drafts. 4) Hit the streets and do some face-to-face marketing. *Inc.com, 10.25.16*

Client Bill of Rights

You have the right to expect and demand complete satisfaction from the information technology and technical services you receive from BSS.
We pledge to deliver exemplary service, on-time and within your budget.

Contest Corner
Who Wants To Win A Gift Card?

This month we are giving away (2) $5 McDonald's Gift Cards. The winners will be chosen at random from all correct entries received by the 16th.

How many counties are there in Indiana?

A) 84 B) 88
C) 92 D) 96

E-mail **Jeff@bssconsulting.com**
with your answers!

Last month's question was: **Which was the first state in the US to recognize Christmas as an official holiday?** The correct answer was D) Alabama.

Kathy Stewart, Ann Hopkins, Lanora Lannan and Betsy Jones were drawn as the winners. Congratulations!

Business System Solutions

Managing Technology For Your Business

BUSINESS SYSTEM SOLUTIONS
1211 Cumberland Avenue
West Lafayette, IN 47906

Phone: (765) 742-3440
Email: bill@bssconsulting.com

Know that the Lord is God. It is he who made us, and we are his ; we are his people, the sheep of his pasture.
Psalm 100:3

CYBER SECURITY

AND THE WAR AGAINST SMALL BUSINESS

EVERYTHING YOU NEED TO KNOW TO KEEP YOUR COMPANY SAFE

EVENT DETAILS

WHEN:
WEDNESDAY, JANUARY 11, 2017

SESSION TIME:
12:00pm-2:00pm

WHERE:
PURDUE TECHNOLOGY CENTER
CONFERENCE ROOM C1-400
3000 KENT AVENUE
WEST LAFAYETTE

PRESENTED BY

Business System Solutions

Shepherd INSURANCE

WITH SPECIAL GUEST SPEAKER
SPECIAL AGENT CRAIG MORINGIELLO
FROM THE FBI

REGISTER AT WWW.BSSCONSULTING.COM/SECURITY
SEATING IS LIMITED SO REGISTER TODAY!