Business System Solutions
May 2017

The BSS Advisor

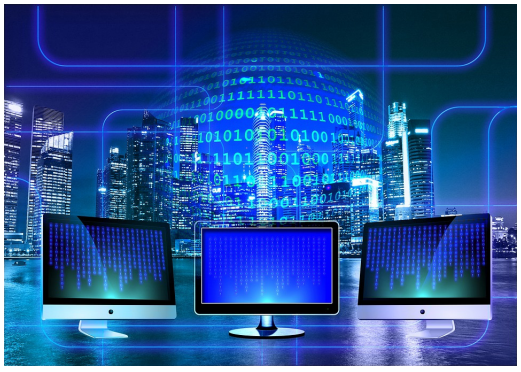
Use This 9-Step Checklist To Ensure Your Data Is Safe, Secure And Recoverable

Inside This Issue:

Summer is upon us… Time for a stroll in the park...softball... fishing...a few rounds of golf…

Yet how could you possibly relax if some random bit of malware, software glitch or cyber-attack catches you off guard just as you're walking out the door? A well-designed secure computer network gives you the confidence that "all systems are go," whether you're having fun in the sun, or just getting things done with your team.

Here's a quick nine-step checklist we use to ensure that a company's computer network, and the data for that business, is safe and secure from disruption, if not absolute devastation:



1. A written recovery plan. Simply thinking through what needs to happen when things go south, and documenting it all IN ADVANCE, can go a long way toward getting your network back up and running quickly if it gets hacked, impacted by natural disaster or compromised by human error.

2. Have a clear communication plan. What if your employees can't access your office, e-mail or phone system? How will they communicate with you? Make sure your communications plan details every alternative, including MULTIPLE ways to stay in touch in the event of a disaster.

3. Automate your data backups. THE #1 cause of data loss is human error. If your backup system depends on a human being always doing something right, it's a recipe for disaster. Automate your backups wherever possible so they run like clockwork.

4. Have redundant off-site backups. On-site backups are a good first step, but if they get flooded, burned or hacked along with your server, you're out of luck. ALWAYS maintain a recent copy of your data off-site.

5. Enable remote network access. Without remote access to your network, you and your staff won't be able to keep working in the event that you can't get into your office. To keep your business going, at the very minimum, you need a way for your IT specialist to quickly step in when needed.

6. System images are critical. Storing your data off-site is a good first step. But if your system is compromised, the software and architecture that handles all that data MUST be restored for it to be useful. Imaging your server creates a replica of the original, saving you an enormous amount of time and energy in getting your network back in gear, should the need arise. Without it, you risk losing all your preferences, configurations, favorites and more.

(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!

IT Security Tip #16: Make THIS Password Different From Everything Else

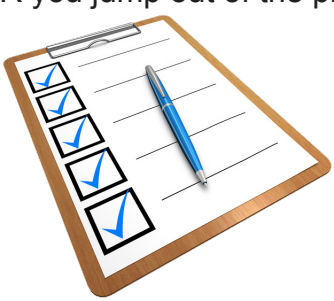
You know you're guilty of it: using the same password for everything. Believe me, I understand how annoying it is to try and remember all those passwords; and if you're using the same password for sites that don't share sensitive information, like a login to a news feed you like to read, then it's generally okay.

HOWEVER, the ONE password you want to keep unique is your e-mail password. If an e-commerce site you've registered at or bought from gets hacked - and you've used the SAME password you usually use for everything to register at the site - you can pretty much bet hackers are going to gain access to your in-box. They'll have your e-mail and your password to the e-commerce site and will use that to hack in. From there, they'll have fertile ground for getting all your data and other passwords.

7. Maintain an up-to-date network "blueprint." To rebuild all or part of your network, you'll need a blueprint of the software, data, systems and hardware that comprise your company's network. An IT professional can create this for you. It could save you a huge amount of time and money in the event your network needs to be restored.

8. Don't ignore routine maintenance. While fires, flooding and other natural disasters are always a risk, it's ever more likely that you'll have downtime due to a software or hardware glitch or cyber-attack. That's why it's critical to keep your network patched, secure and up-to-date. Deteriorating hardware and corrupted software can wipe you out. Replace and update them as needed to steer clear of this threat.

9. Test, Test, Test! If you're going to go to the trouble of setting up a plan, at least make sure it works! An IT professional can check monthly to make sure your systems work properly and your data is secure. After all, the worst time to test your parachute is AFTER you jump out of the plane.



Be certain that you have all 9 steps fully covered with our FREE Disaster Recovery Audit.

Contact us at (765) 742-3440 or bill@bssconsulting.com to schedule our Disaster Recovery Audit FREE of charge, now through May 31. Contact us TODAY to get scheduled!

"IT can be very stressful. It's normal to feel overwhelmed. Say, while you're here, I've been having this problem..."

 WWW.ANDERTOONS.COM

FACT FILE

DID YOU KNOW?

- Jackie Chan dubbed the lines for the Beast in the Chinese translation of Disney's animated classic Beauty and the Beast, and he also sang all the Beast's songs in Mandarin.
- There is a scientific measurement for the 'risk of death' of any action: the micromort. If an activity is rated as one micromort, you would have a one in a million chance of dying while doing it. Running a marathon is ~7 micromorts, sky diving is 10, and climbing Mount Everest is 40,000!
- Finnish police found a dead mosquito while searching a stolen car. They tested the blood from the mosquito's last meal and used it to identify the thief.
- In captivity, ravens can learn to talk better than some parrots. They also mimic other noises, like car engines, toilets flushing, and animal and birdcalls. Ravens have been known to imitate wolves or foxes to attract them to carcasses that the raven isn't capable of breaking open.

Client Bill of Rights

You have the right to individual attention and dedication.

We pledge to provide prompt, courteous, and efficient service by acknowledging your request within an hour, keeping appointments, and with great communication.

Ransomware Attackers Are Setting Their Sights On Small Businesses

Do you think your business is safe from a ransomware attack? It isn't.

This was indeed the case that when ransomware first burst onto the scene. Hackers were targeting very large institutions, seeming to favor the health care and insurance industries. But that is now changing, at least according to a recent report published by Datto.

The security firm surveyed European IT Service providers to get a sense of the shifting landscape, and made a grim discovery. Based on their survey results, fully 87% of IT service providers indicated that their small and medium-sized business customers had been targeted by a ransomware attack during the last twelve months.

Four out of ten said that they had been hit more than once in that same period.

While the numbers may not match precisely with US figures, there's no reason to suspect that they'd be radically different, which represents a disturbing trend.

It is unclear what's driving the shift. It could be simply that most of the low-hanging fruit has already been plucked from the land of corporate giants.

Also, as a direct result of those early ransomware attacks, big companies ramped up their spending on digital security, making their networks significantly harder targets than they were just a few short years ago.

Perhaps most disturbing in Datto's findings was the fact that in almost half (47%) of cases where the ransom was paid, the promised unlock key to restore the company's files was never delivered, or didn't work, and the company wound up losing their data and the money they paid in ransom.

With a typical ransom running between $500 and $3500 (and sometimes more), it's a big problem, and it's getting worse by the month. If your digital security isn't as robust as you'd like it to be, now is the time to do something about it.

If your own staff is stretched too thin to bolster your defenses, or if you're not sure how to proceed, call us today at **(765) 742-3440**. You'll speak with an expert in the field who can assess your current situation and put you on the path toward greater security, which will give you greater peace of mind.

Last month's question was: **What was the original state capital of Indiana? The correct answer was B) Corydon. It was the first capital of Indiana from 1816 to 1825.**

Debbie Herron was drawn as the winner. Congratulations!

TECH TALK

Is your in-car GPS necessary anymore? Smartphones offer turn-by-turn navigation, satellite-tracked speed readings, voice guidance and real-time, crowdsourced traffic alerts. So why dish out another 300 bucks for your own on-dash, in-car system? Well, those in-car systems have come a long way too… Having voice-command capability, Bluetooth connectivity, geo-based recommendations and a large fixed screen might be reason enough. But if your phone's monthly data allotment and battery life concern you at all, that in-car GPS, with its own data and power sources, starts looking pretty good. And with features like a streaming dash cam and sensor that warns you if you're following a car too closely, in-car GPS is definitely worth a second look.
DigitalTrends, 02.24.17

Get totally weird with new Virtual Reality (VR) tools. You may not have a clue about how to draw at all, much less in 3-D. Doesn't matter… Whereas VR used to be a tool for techies, now amateurs can get in on the act. A-Frame by Mozilla, for instance, lets you easily type in commands that place 3-D objects like blocks, balls and more into a VR scene you create. Tilt Brush lets you paint in the air wearing a Google Vive headset. And Second Life inventor Philip Rosedale is building software that lets you invite friends into a VR world you design. Most of what any amateur creates will likely be grotesque, ugly or flat-out lame, but somewhere in all that mess, amazing new products will be born. *Wired, 02.24.17*

Contest Corner
Who Wants To Win A Gift Card?

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

Jim Davis, the creator of Garfield, was from which Indiana County?

A) Lake
B) Monroe
C) Hamilton
D) Marion

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

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

"The Lord your God is with you, the Mighty Warrior who saves. He will take great delight in you; in his love he will no longer rebuke you, but will rejoice over you with singing." Zephaniah 3:17 NIV

From Bill's Desk

Wow, it's May and we are a third of the way through 2017! One of the things we keep hearing in our industry news is that this year we will again see a huge increase in ransomware attacks. At BSS, we feel our multi-layered approach to security, from a great Backup and Disaster Recovery to the many layers of protection like antivirus/firewall/DNS blocking/ antimalware, and finally user education has enabled us to totally avoid viruses and ransomware over the past year and a half. We tell our clients to never open attachments or click on the links, unless absolutely sure it is safe, and to call us if unsure. For our clients we offer a seminar for users to help them understand the dangers of the cyber world, and how to avoid being part of the problem. If you are interested please give me a call so we can discuss the details.

Business System Solutions Is Your Total IT Partner
www.bssconsulting.com

What Our Clients Are Saying

"I Feel More Secure Than Ever"

BB&C

-Roger Bennett
Attorney/Partner
BB&C

"BSS' remote support permits very punctual response to many small issues on workstations. We've got better remote access now than ever through a secure VPN, it sure is nice to be able to commandeer my workstation from outside the office. I also very much like the way you've assigned access rights on our server. I feel more secure than ever that nobody can get access to information they're not supposed to see. It is nice to say 'we need 4 new workstations; please configure and quote them for us'. I've reduced my time on our network a lot and can practice more law!"