BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time. • **September 2017**

Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

Are You Prepared for a Natural Disaster?

Let's face it… no one likes to think about bad things happening to them, much less planning for them – Disaster Recovery Planning is one of those "important, not urgent" action items that (unfortunately) gets pushed to the back burner. September is National Preparedness Month and with the recent hurricanes, Hugo and Irma, there is no better time than now to review your Disaster Recovery Plan (if you even have one) and make updates as needed. Disasters don't plan ahead, but you can!

How quickly a company is able to get back to business after a terrorist attack, a tornado, a fire, or a flood often depends on emergency planning and preparation done before the disaster strikes. Federal Emergency Management Agency (FEMA) highlights three steps to Business Disaster Preparedness, called "The Ready Campaign"

1) Plan to Stay in Business
2) Talk to Your People
3) Protect Your Investment

These steps underscore how important it is for businesses to document their property/ equipment, back up business-critical information, and put a response team in place.

And it's not just natural disasters you need to plan for. Things like hardware failure, software corruption, virus/hacker attacks, internet connectivity outage, no access to your office building (crime scene, pest infestation, fire, etc.), theft of physical devices, and even human error (erasing data accidentally or intentionally) can cause damage, interruption or loss to your company's operations, systems and data for a period of time that would be determined detrimental to your company's growth or survival.

In a study by Cummings, Haag & McCubbrey in 2005, of companies that experience a major data loss without having a solid disaster recovery plan in place, ONLY 6% survive; 43% close their doors immediately and 51% limp along and eventually close within 2 years. According to FEMA **90% of smaller companies fail within a year unless they can resume operations within 5 days of a disaster**. And the situation is getting worse as more and more companies store – and rely on – digital information and systems to serve customers and keep the doors open.

A Disaster Recovery and Preparedness Plan, and more specifically an **IT Disaster Recovery and Preparedness Plan**, is critical in making sure your company can survive and thrive.

To assist you in creating a *IT Disaster Recovery and Preparedness Plan* for your company, we've created a resource page including Disaster Planning Essentials, a Disaster Planning Checklist, and a FREE Disaster Recovery Assessment: www.bssi2.com/disasterprep

The Lighter Side….

Old Golfer Speaks Out:

"We had a power cut at our house this morning and my PC, laptop, TV, DVD, iPad & my new surround sound music system were all shut down.

Then I discovered that my mobile phone battery was dead. To top it off it was raining outside, so I couldn't play golf.

I went into the kitchen to make coffee and then I remembered that this also needs power, so I sat and talked with my wife for a couple of hours.

She seems like a nice person."

The End (of Windows 7 SBS) is Near, Prepare

Written by Chris Fedor

Yes, the end is near. Not quite an apocalyptic event, despite what events in Texas and Flordia seem to portray, but a significant technology end that needs to be planned. Many of you may have missed **Microsoft's announcement that it is ending extended support for Windows 7, SBS2011 and Server 2008 R2, SBS2011** January 14, 2020. Now you may say to yourself, "Hey that is 2 years off, I don't need to worry about that now." Well, I challenge that thinking. While the end of Microsoft extended support is not a cataclysmic event and your machines will not all of a sudden stop working, it means that Microsoft will no longer be offering patches and fixes for Windows 7 known vulnerabilities. Fixes that our lovely hacker friends could and will exploit to their advantage and put your company at risk. Now is the time to think about what you have that will be effected by this announcement, and what you will need to do when it arrives.

You don't want to be caught in 2020 or 2021 having to replace 1 or more servers and 5, 10, 20 computers all at the same time. No business, wants to have a large expense hitting in the same year. It just doesn't make good financial sense. So, start now. First gather an inventory of what you have and what operating system it is running. Then, look at the software you are running. Do you have the media to reinstall? Is the software even supported on Windows 10 or Server 2016? Software upgrades can be just as costly as the physical hardware. Planning the software is as invaluable as the physical pc upgrades.

Next you need to look at timing, are there deadlines that must be met and when, so installs do not negatively impact those dates. Is there a slow period, where server work or pc replacements would not impact production schedules. Then develop a replacement plan, maybe 1 or 2 new computers each quarter spread over the next 2 years makes sense to you. Or maybe this year move the pc's and next year the servers. By planning these things out the choices are yours and on your schedule and pace. We have seen people leave server and critical machines in place well after their life cycle has passed by only to be caught with high weekend and afterhours fees because those machines have failed and must be replaced NOW. Understandably, these situations are different to a degree, but emphasize planned replacements are on average cheaper than the emergency unexpected, unplanned for types.

It was Ben Franklin, who coined the phrase, "By failing to prepare, you are preparing to fail". It is as true a statement now as it was in his day. The time spent today planning for the end of Windows 7, SBS2011, and Server 2008r2, will be far less than the cost of time and material waiting for the last minute.

More Common Than Mother Nature's Disasters, What Will You Do When This Disaster Hits Your Business?

In today' s world of rampant cybercrime, every savvy business owner knows the necessity of locking down their data. However, we find that the cyber security technologies used by the vast majority of businesses are woefully out of date. Sure, your current solution may have worked great, but digital threats to the safety of your company are constantly evolving. Criminals will eventually attempt to breach your data — and your barriers are not as secure as you might think.

Before World War II, the Germans developed a technology that would prove to be a key player in the conflict: its family of infamous Enigma machines. These devices, about the size of a small microwave, were composed primarily of a typewriter and a series of three or four rotors. By using a set of rules contained in a corresponding codebook, German soldiers would use the machine to encode vital messages to be sent covertly over the airwaves. The number of potential permutations — and thus solutions — for the code was in the tens of millions. The Germans were confident that the code could never be broken and used it for a vast array of top-secret communications.

The code's impenetrability didn't last. Via photographs of stolen Enigma operating manuals, the Polish Cipher Bureau reconstructed one of the stubborn Enigma machines, internal wiring and all, enabling them to decrypt the Wehrmacht's messages from 1933 to 1938. Facing an impending German invasion, Poland decided to share these secrets with the British. But, at the outbreak of the war, the Germans increased the security of the Enigma initiative by changing the cipher system daily. In response, a British code-breaking team, led by genius English computer scientist Alan Turing, constructed primitive computers, known as "bombes," that allowed them to decrypt the incredibly complicated ciphers faster than ever before. But it wasn't until the capture of the U-110 warship and the seizure of its Enigma machine and codebooks that the British were able to decrypt the most complicated cipher of the war, the Kriegsmarine Enigma.

The information gleaned from these decrypts are believed to have shortened the war by more than two years, saving over 14 million lives.

Just like you, the Germans believed the systems they had put in place to defend their secrets were impenetrable. And it's true: the system had few cryptographic weaknesses. However, there were flaws in German procedure, mistakes made by Enigma operators, and failures to introduce changes into the Enigma formula — along with the Allied capture of key equipment and intelligence — that ultimately allowed the Allies to crack the code once and for all.

Take this as a cautionary tale: the most advanced, complex cryptography system in the world became obsolete within 10 years. The same goes for your potentially outdated cyber security measures.

Though they may not be led by Alan Turing and his crack team, you can bet criminals are constantly chipping away at the defenses of even the most powerful firewalls. The arms race between cyber security companies and cybercriminals rages on behind the scenes, and you can bet that they've already cracked your business's "Enigma." Just look at the massive European cyber attack this past June, which infected computers from over 27 companies across the continent, including those of the largest oil company in Russia, with ransomware. The unimaginable cost of that attack is something you certainly don't want your business to shoulder.

As technology evolves, so does crime. New threats arise each and every day. While solutions are available (and needed), they are notably absent in older software developed at a time before these constantly morphing attacks even existed.

Once the enemy has found a way to pick your lock, you need a new lock. Luckily, you have your trusty IT provider, constantly on the lookout for cutting-edge solutions that protect our clients from even the nastiest malware.

Don't be like the Germans. Constantly look at options to upgrade to more robust, better cyber security to defend yourself from the bleeding-edge hackers, and sleep safe knowing your business is secure.

September 2017

35 Aztec Court
South Barrington,
IL 60010

(312) 752-4679

www.bssi2.com

Gadget of the Month

Building A Smarter Shower

The cutting-edge U by Moen Smart Shower is looking to revolutionize your shower experience. With digital valves and a corresponding controller, the U by Moen can make any shower a lot smarter.

After users install the digital valves and controller — a task that takes a few tools and a little bit of handiwork — the U by Moen allows them to sync their showers with their smartphone. The system then makes it easy to customize the showering experience, choosing the perfect temperature and saving preferences for future use. Start the shower remotely, and it will let you know when it's ready, automatically shutting off until you step in. Available for showers with either two or four outlets, the U by Moen is the perfect addition for those looking to digitize every aspect of their home.

Helping Out After Disasters, How to Avoid Scams

Knowing where to give your donation dollars is more confusing than you may think. Moreover, tragedies like Hurricane Harvey tend to bring out both the best and worst in humanity.

"Low-life cyber scum are exploiting this disaster using fake social media accounts," Arizona Attorney General Mark Brnovich said in a statement warning citizens of scammers attempting to profit off the victims of Harvey. "When a natural disaster strikes, many of us ask, how can we help? Giving is good, but it's important to donate to a legitimate charity that has experience helping victims quickly."

Before giving money to an organization, do your research.

Charity Navigator (www.charitynavigator.org/), which identifies worthy charities, has a list of organizations responding after the Hurricane Harvey storm. Its database is a good starting place to research nonprofits.

The Internal Revenue Service has search tools that reveal whether an organization is eligible to receive tax-deductible charitable contributions: www.irs.gov/charities-non-profits/exempt-organizations-select-check

"Be wary of charities that spring up too suddenly in response to current events and natural disasters," the Federal Trade Commission (F.T.C.) website says. "Even if they are legitimate, they probably don't have the infrastructure to get the donations to the affected area or people."

If you suspect an organization or individual is engaging in fraud, you can report it to the National Center for Disaster Fraud.