BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

On the Lighter Side

A story from Tumbler:

When I was a kid, I was always excited to learn new vocabulary. When I was in first grade, my teacher taught me that "shin" was another word for leg.

Later that day, I was walking with my mom, when I tripped and hit my leg on the ground really hard. I yelled out "OW, MY SHIN" although my mom heard "OW, MY SH*T." She started yelling about how that was a bad word and we didn't say that word, and she was going to wash my mouth out with soap. I was a crying, bawling mess of a child, to the point I was doing that weird cry, stutter, hiccup noise. She paused in berating me and said "Who taught you that word?!" Of course, I told the truth and said "M-m-my teacher t -t-t-taught me that word!" and she started ranting about how she was going to call the school and get that teacher yelled at.

I tried to explain, "T-te-teacher said that shin meant leg I'm SO SORRY ILL N-N-NE-ne-never say it again." My mom got quiet and realized her mistake. "… What did you say?"

Of course I started crying harder and I said "NO it's just a test you're going to wash my mouth out with soap again."

When I finally calmed down enough to say it again, my mom apologized and to this day I always say "shin" loudly just to see her face blush.

You NEVER See It Coming! But Once It Hits, Everyone Says, "I Wish I Would Have_____"

A year ago, no one could have predicted that countless businesses would shift to a remote work model. The pandemic hit hard and fast, and small businesses had to think on their toes. Many had only a few weeks to adapt. It was stressful and extremely challenging.

Looking back on it, many SMBs wish they'd had a plan in place that would have made things easier. When the pandemic hit in February/March 2020, SMBs had to absorb the huge cost of getting their employees up and running off-site. Not only was it costly, but it also took a lot of coordination and on-the-fly planning. This meant things slipped through the cracks, including cyber security.

As they say, hindsight is 20/20. You may wish you had a plan in place or had more time, but you didn't. A vast majority didn't. However, you can still plan for the future! While you never know when disaster is going to strike, you CAN be prepared for it. Whether that disaster is a pandemic, flood, fire or even hardware failure, there are steps you can implement today that will put you in a better place tomorrow. Here's how to get started.

Put Your Plan Into Writing.

First and foremost, you should have a standard operating procedure to call on should something go wrong. For example, in early 2020, many SMBs didn't have a security plan in place, let alone a remote work security plan. They had to make it up as they went, which just added to the challenges they were already experiencing.

To get over this challenge, work with an experienced IT services company or managed services provider (MSP) to put together a plan. This plan should include a cyber security protocol. It should define what malware software employees should be using, what number they should call for 24/7 support, who to contact when they receive suspicious e-mails, how to identify suspicious e-mails and so on.

More than that, it should outline exactly what needs to happen when disaster strikes. Pandemic? Here's how we operate. Fire? Here's what you need to know. Hardware failure? Call this number immediately. The list goes on, and it can be pretty extensive. This, again, is why it's so important to work with an MSP. They've already put together plans for other SMBs, and they know where to start when they customize a plan with you.

Invest In Security And Backups.

While every business should have network security already in place, the reality is that many don't. There are a ton of reasons why (cost concerns, lack of time, lack of resources, etc.), but those reasons why aren't going to stop a cyber-attack. Hackers don't care that you didn't have time to put malware protection on your PCs; they just want money and to wreak havoc. As a matter of fact, they are counting on that; it makes it easier for them to hack you.

~ Continued on next page...

… continued from previous page.

When you have IT security in place, including firewall protection, malware software, strong passwords and a company-wide IT security policy, you put your business and all your employees in a much better place. All of this should be in place for both on-site employees and remote workers. With more people working from home going into 2021, having reliable IT security in place is more important than ever before.

On top of that, you should have secure backups in place. Investing in cloud storage is a great way to go. That way, if anything happens on-site or to your primary data storage, you have backups you can rely on to restore lost or inaccessible data. Plus, having a solid cloud storage option gives remote employees ready access to any data they might need while at home or on the go.

Where Do You Begin?

Some SMBs have the time, money and resources to invest in on-site IT personnel, but most don't. It is a big investment. This is where partnering with an experienced IT services firm can really pay off. You may have employees in-office or you may have a team working remotely – or you may have a mix of both. You need support that can take care of everyone in your organization while taking care of the data security of the business itself. This is where your IT partner comes into play. They are someone you can rely on 24/7 and someone who will be there for you during a pandemic or any other disaster.

Production Vs. Connection – The Ailment

Recently, I had what we like to call an "aha moment" while listening to a sermon one Sunday. The minister made the observation that our society as a whole has swung to the extreme side of productivity at the expense of our connections. It hit me that this is one of the greatest ailments we see as coaches with our member companies and leaders, especially as of late.

Culture Appreciation Connection

We know the best-performing companies are those that devote significant effort to creating a culture that their team members want to be a part of. And where does that culture come from? People crave appreciation in the workplace – and we're talking sincere, heartfelt appreciation, not the casual "pat on the back" or quick "thanks" in passing. Real appreciation only occurs if there is a real connection between people. Connection is valuing the other person more than yourself or having an "others first" mindset. It takes effort, vulnerability and emotion. True culture cannot exist without both of these key elements.

The Ailment

Unfortunately, in our "all about me" culture, connections tend to be shallow and unemotional. It's not what can I do for you, it's what can you do for me. As a society and in business, we have become so laser-focused on overachievement and beating the competition that our connections receive little attention. Especially today, when companies are striving to get back on their feet, push out new offerings and make up for lost time from the pandemic, connections are starving due to the demands of winning.

But At What Cost?

There have never been higher instances of job discontentment, disconnected families, depression, suicide and overall lack of joy. Our extreme focus on production and achievement has come at a huge cost to society. Extremes at either end of the pendulum never end well.

So, Now What?

Back to our coaching perspective, I think we have it right when we help our companies focus on culture by viewing their team members as human beings and not just a means to productivity. In addition, we all know that you cannot truly separate the business side from the personal side and that you have to be equally intentional in both areas to create the life you want, which involves real connections to who and what we love.

It's time to swing the pendulum back, ease off the production pedal and give more attention to treating each other with compassion and putting others first. It may seem strange, but the companies that have done this well typically outperform on the production side, too, because connection is a great motivator for betterment – both personally and professionally.

Gee, maybe there's really something to the old Golden Rule thing.

David Pierce spent the first 30 years of his career in the corporate world. As a CPA, he spent a decade with Deloitte and PcW, and another 20 years in a C-level post in regional banking. He also launched one of the first stand-alone online banks in the US. As an entrepreneur, he eventually said goodbye to the corporate world and started his own consulting firm, and became a Four Decisions Certified Gazelles International Coach and a Petra Coach.

SolarWinds: The Breach That Has Made Worldwide News

By Scott Bernstein

What Happened

As you probably know by now, as it has been all over the news, there have been some very high profile cybersecurity breaches at governmental agencies as well as large corporations. It was reported by The Hill on 1/5/21 that U.S. intelligence agencies (FBI, NSA and CISA) have formally accused Russia of being linked to this breach. The breaches involved FireEye and SolarWinds Orion management services and started in February or March 2020. There are 18,000 entities potentially affected by this breach. SolarWinds' customer listing (with over 300,000 customers worldwide) includes over 425 of the US Fortune 500, all top ten US telecom companies, hundreds of universities and colleges, all five branches of the US Military, the US Pentagon, the State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States.

We want to let our clients know that none of these applications or tools are used by BSSi2 or on of our clients' networks by BSSi2.

The Cybersecurity & Infrastructure Security Agency (CISA) has stated "CISA has determined that this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations… This is a patient, well-resourced, and focused adversary that has sustained long duration activity on victim networks... Not all organizations that have the backdoor delivered through SolarWinds Orion have been targeted by the adversary with follow-on actions."

Microsoft President Brad Smith state "This latest cyber-assault is effectively an attack on the United States and its government and other critical institutions, including security firms… This is not espionage as usual." 80% of those affected are in the US with at least 7 other countries identifying victims.

What is being done

This all being said, nobody is standing still on this issue. Major technology companies are creating automatic updates to be pushed out to guard against and eradicate the infections (sorry, I cannot report on every vendor).

- As noted in an article by GeekWire on 12/16/20, "Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach". We provide a link to this article at the end of the email. We have checked several systems and see these updates are being pushed out. Microsoft says they have neutralized the infection before any major damage was done.
- Palo Alto, on 12/14/20 stated it is updating its subscription software. We have checked several systems and see these updates are being pushed out. "As of the time of writing, based on signatures and observables that have been released, Palo Alto Networks customers are protected across its product ecosystem, with specific protections deployed or being deployed in the products and subscriptions for the Next-Generation Firewall (NGFW)".
- Web browser Mozilla has released security updates to FireFox & Thunderbird
- Apple has released security updates for multiple products
- Adobe released security updates for Acrobat and Reader
- SolarWinds has stated: "First, we want to assure you we've removed the software builds known to be affected by SUNBURST from our download sites."
- VMware claims its systems have not been "abused" by this breach but recommends all customers apply security updates available.
- Microsoft, FireEye, and GoDaddy also collaborated to create a kill switch for the SunBurst backdoor distributed in the SolarWinds hack.
- Cisco (for all their product lines, include OpenDNS/ Umbrella): "At this time, there is no known impact to Cisco products, services, or to any customer data."

Concluding thoughts

As reported by Nextgov web site on 1/7/21, part of the breach was caused by hackers guessing at passwords using common hacker techniques and password spraying. AND SolarWinds themselves used a password for its update service that anyone could guess. You know where we are going with this:

Don't use the same password at more than one site and make them complex!

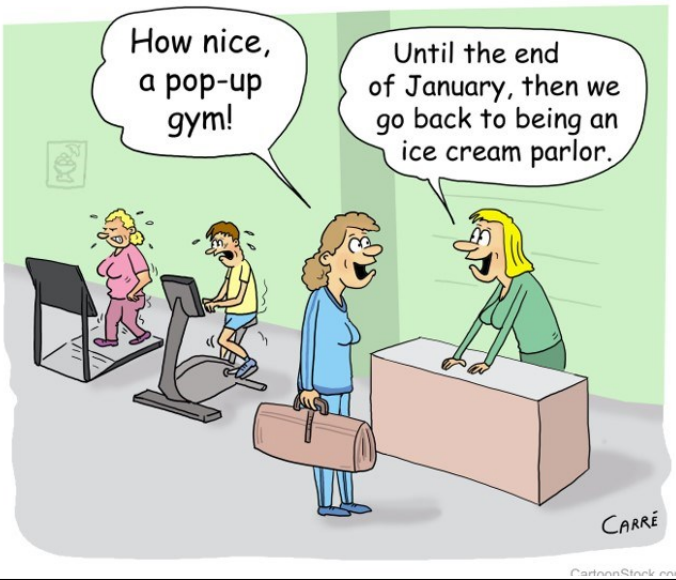
No one single, or group of, solutions will guarantee you are 100% protected from breaches and infections. As this incident shows, even the biggest, best entities with money to throw at security can be hacked if the perpetrator is determined to get you. The key lesson is most hackers are neither this persistent nor this sophisticated to continue an attempted breach if they see adequate layers of protection in place. Be sure you are a company that makes it difficult to get to your network and staff. Give us a call if you need guidance and assistance with this.

January 2021

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Good intentions last a month on average



Shiny New Gadget of the Month

FitTrack: A Revolutionary Scale Lets You Look Inside Your Body

Right now, countless people have gotten lax on their New Year's resolutions and given up on their goals. One of the most popular resolutions is to get fit. It is also one of the most challenging ones to see through to the end. The FitTrack smart scale is here to make that a little less challenging!

FitTrack has earned its designation as a smart scale. It does much more than tell you your weight. With a number of other sensors, as well as data you input into the FitTrack app, it can tell you all sorts of things. Yes, it will tell you your weight, but it will also tell you things like body mass index, muscle and bone mass and hydration levels, to name just a few. In total, it can track 17 key health insights.

As you work toward your fitness goals for the year, don't miss out on a companion that will give you crucial data along your fitness journey. Discover more about FitTrack at bit.ly/2VOg7Vs.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc