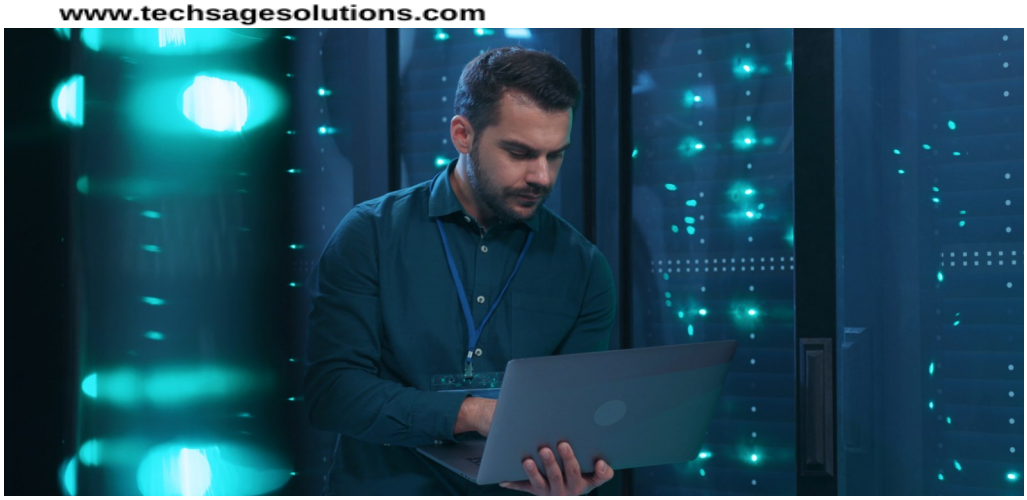
TECHSAGE
Monthly Newsletter

Tips & Awesome Info for Technology
www.techsagesolutions.com

Your monthly newsletter provided by John Hill, President and CEO of TechSage Solutions



Inside This February Issue

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

INSIDER THREATS: A guide to understanding, detecting and preventing insider security incidents

Shiny New Gadget of the Month

The Worst Passwords Of 2020

Production Vs. Connection – The Ailment And The Cure

Free Executive Zoom Webinar Thursday, February 18th at 11:00am cst Easy IT Compliance for the Defense Industrial Base (DIB)

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

Continued on pg.2

Continued from pg.1

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.

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.

> **"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."**

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.

INSIDER THREATS: A guide to understanding, detecting and preventing insider security incidents

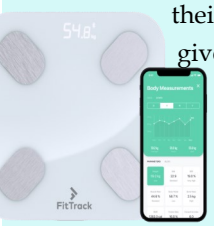
Data protection regulations require your business to assess all possible threats to the sensitive data your business stores or manages. While most businesses tend to focus most of their attention on external threats, they often overlook insider threats that exist right under their collective noses.

While your employees may form the first line of defense against cyberattacks, all it takes is one of them acting out of line to cause damage to your business. To put this into perspective, Verizon's 2020 Data Breach Investigations Report stated that 30 percent of breaches involved internal actors.

Find out more by downloading your free e-book
https://www.techsagesolutions.com/insider-threat-ebook-request/

SHINY NEW GADGET OF THE MONTH

FitTrack: A Revolutionary Scale Lets You Look Inside Your Body

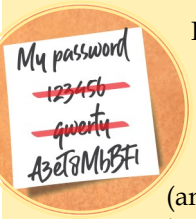


Right now, countless people have gotten lax on their New Year's resolutions and given up on their goals. One of the most popular resolutions is to get fit. It is also one of the most challenging ones to see through to the end. The FitTrack smart scale is here to make that a little less challenging!

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.**

The Worst Passwords Of 2020!



Password manager NordPass recently revealed the worst passwords of 2020. The list included several passwords that were on the list in 2019 (and the year before that). These are passwords that hackers and cybercriminals LOVE. It makes getting into accounts super-easy.

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678

One of the reasons these passwords are so frequently used is because they are easy to remember and they require little effort to type. As a general rule of thumb, the easier a password is to type (like 123456) or remember, the easier it is for a hacker to crack. Never use these passwords!

Production Vs. Connection – The Ailment And The Cure

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.

FREE EXECUTIVE ZOOM WEBINAR

Thursday, February 18th at 11:00AM cst

Easy IT Compliance for the Defense Industrial Base (DIB)

ARE YOU STRUGGLING to figure out how to get certified at the CMMC level you need to win new DoD contracts and keep the ones you currently have?

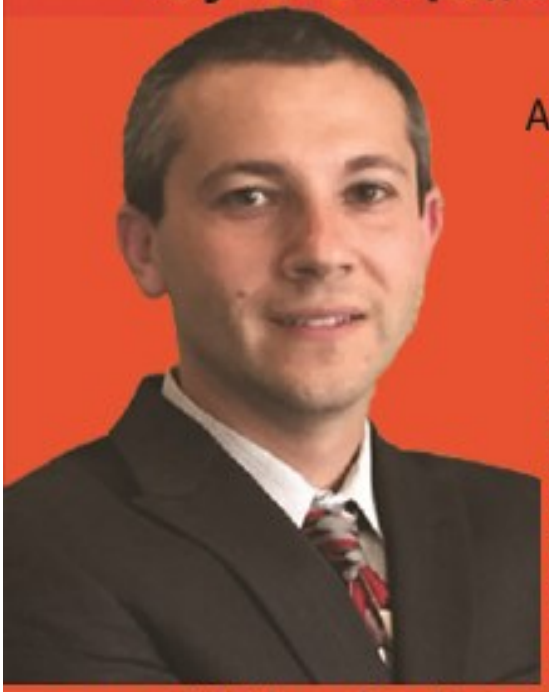
ONCE YOU'VE been certified how do you stay certified, stay secure and stay compliant with CMMC requirements and still have time to effectively run your business?

Find out how you achieve compliance and even more importantly how you stay compliant to avoid any disruptions to your business.

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

TechSage Solutions

Register at https://www.mycmmcjourney.com/dibcompliance



About Our Speaker

Max has been a pioneer in the managed services industry since the late 1990s. He currently serves as General Manager of Compliance Manager for Kaseya and is responsible for Kaseya's Compliance go to market strategy. Prior to rejoining Kaseya, Max served as Chief Revenue Officer of CloudJumper (acquired by NetApp), where his responsibilities included running all aspects of the company's sales operations, managing and developing an MSP channel and building a world-class sales organization. Max was the director of strategic accounts for Kaseya where he was recognized four years in a row for sales excellence, winning the Chairman's Cup for outstanding sales success. Max began his career at USWeb as a founding member of that company's managed service division. He has also held Architect at IBM. Max holds a BS in Computer Science from American University and an MBA from American University and an MBA from the University of Maryland - Robert H. Smith School of Business.