TECHSAGE TECH TALK

"Insider Tips To Make Your Business Run Faster, Easier, and More Profitably"

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

What's Inside:

Employees Keeping Your Data Safe? Don't Count On It.

One morning late last year, an unemployed man was making his way across London, heading to the library to continue his job search. But on the way, he encountered something peculiar: a USB stick, peeking out among the fallen leaves and shining in the morning sun. Not thinking much of it – and perhaps afflicted with a morbid curiosity – he popped the device into his pocket and continued on his way. Once he made it to the library, he connected the USB to a computer to check out its contents. As he clicked around, he realized with a shock that this was a treasure trove of security information for the Heathrow International Airport: 174 folders packed with maps detailing CCTV camera locations, labyrinthine tunnels snaking below the building and even the exact route the Queen takes when she uses the airport.

Understandably worried, the man quickly ejected the device and brought it – for some reason – to local tabloid the *Daily Mirror*. Today, despite a full-scale security investigation by the airport and the scrutiny of dozens of police and security experts, it's still unclear just where this extremely sensitive data came from. However, all signs point to the USB drive being dropped by either a hapless employee carrying around a national security concern in their pocket or a less-hapless employee looking to instigate a national security crisis.

Either way, the story hammers home a vital point: whether you're an international airport hosting more than 70 million travelers each year or a small business with less than $10 million in annual revenue, your biggest security risk isn't some crack team of hackers – it's your employees.

Continued on pg.2

Continued from pg.1

Sure, you may chuckle at the idea that any of your employees would actively wish your organization harm. But we're willing to guess that you probably underestimate the wrath of an employee scorned. Even if you treat your team better than any boss in the world, they are still human – which, of course, means they're going to make mistakes from time to time. And when considering the cyber security of many SMBs, "time to time" actually means every day, leaving huge openings in your digital barriers. These errors don't much matter, really – until the day that a hacker turns an eye toward your business and immediately realizes the laughable security gaps your team is leaving for them to exploit.

The thing about cyber security is that it's a lot more complicated than most people are willing to admit. Today's digital landscape is fraught with hazards, a thousand little mistakes to be made at every step, resulting in a million workarounds for cyber criminals to use. Even the most tech-savvy among us probably don't know everything about cyber security, and very few have as much knowledge as the hackers on the other end of the equation. When you consider the uncertainty and potential miseducation of your employees, many of whom probably know next to nothing about cyber security, you might start to feel a little panicked.

The battle against digital threats can seem like an endless slog – a war that the good guys seem to be losing – but luckily, when it comes to the security of your business, there are ways to batten down the hatches without dropping a ton of cash. For instance, start with your biggest vulnerability: your team. When a new employee joins your organization, they should go through a thorough cyber security training. Their welcome forms should include comprehensive rules about security policies, from using strong passwords to how they should respond to potential phishing attempts. Deviating from these policies should come with serious consequences.

> **"Your biggest security risk isn't some crack team of hackers—it's your employees."**

As for your existing employees, train them up! We can help you build a robust education program to get every single member of your organization up to speed on the most imminent cyber security threats. But even then, cyber security isn't a one-and-done kind of thing; it requires constant vigilance, regular updates on the latest trends and a consistent overall commitment to protecting your livelihood. Without training and follow-up, even the most powerful of cyber security barriers are basically tissue paper, so put some thought into your team in addition to your protections, and you can drastically increase the safety of the business you've worked so hard to build.

Shiny New Gadget Of The Month:

An Indoor, No-Hassle Cookout: The Kenyon City Grill

As we draw close to the end of summer, many of us are stowing our grills in preparation for the cooler months. Others never had a grill in the first place, banned by their lease from ever doing any sort of grilling. Regardless of the reason, pretty much everyone bemoans a grill-free existence, even if it's only for a few months. Enter the Kenyon City Grill, a handy grill for those of us who need to stay inside to cook up a hot dog or hamburger. With some complicated engineering tricks, the grill can cook anything you throw at it with virtually no smoke, far exceeding the requirements of city fire codes and preventing you from getting smoked out of your kitchen. Its $475 price tag may seem a little steep, but consider the convenience of grilling right from your kitchen, all year long – even if you're in an apartment! – and you can quickly see the benefits.

What It Takes To Succeed

If there's one characteristic common to all successful entrepreneurs, it's that they are notoriously difficult to keep down. Even through the most embarrassing failures and toughest trials, they learn from their mistakes and keep pressing on.

Take Gary Nealon, for example. Before he was founder of the e-commerce consulting firm Nealon Solutions, he built multiple multimillion-dollar businesses from the ground up – but not before experiencing a nasty failure that put him into bankruptcy. Now, he's compiled his hard-earned lessons into a book called Notes to a Young Entrepreneur, hoping to equip newbies with the wisdom he wishes he'd had when he first started out. In it, he emphasizes the important lesson that no matter how hard an entrepreneur falls, they need to be able to actively learn from their mistakes and continue moving forward.

8 Tendencies Of Bad Decision Makers

At one point in my career, after I'd started, grown and sold a couple of businesses, I thought I knew everything there was to know about making good decisions. After all, I was a success! But it took me a few years to realize that, in many respects, I still had a lot to learn about making the best calls. Here are the lessons I learned the hard way back then about the tendencies and motivations of people who are making the worst business decisions of their lives.

BASING DECISIONS ON EGO
If you think you know it all and that your expertise in a narrow field will translate to every other field, you're just flat wrong. Assemble a team of folks whose experience rounds out your own and reap the benefits of multiple perspectives.

RELYING ON THE MOMENTUM EFFECT
There's certainly some truth to the belief that past events can predict future events. The problem with this thinking, though, is that the world is constantly evolving. If you're sticking with the tried-and-true and refusing to look at other options, you're likely to misstep.

BEING LAZY
Entrepreneurs have to be hungry and curious. Make sure you're looking at the whole picture, and at both the negatives and positives of any potential decision.

BEING INDECISIVE
If you're putting off making a choice, you can end up limiting your options down the road. You may be right, you may be wrong, but don't let yourself get cheated out of success.

GOING IT ALONE
You simply can't understand all the options and complexities of a given situation on your own. Sometimes the best results come through compromise with a team you've assembled.

EXECUTING POORLY
Making a decision is only 10% of the process. The other 90% is the actual execution of that decision. If you fail to communicate the reasons for your decision to your staff, neglect to plan or follow up, or simply drop the ball, you're not getting the job done. Make sure you implement your changes in a thoughtful, logical way.

SEEING THE TREES RATHER THAN THE FOREST
Good decisions are made with the big picture in mind. If you're focused on putting out fires or only thinking about next week, you're not going to be able to adequately plan ahead. Leave the short-term decisions to your trusted staff and devote your energy to the long term.

NOT BALANCING YOUR SOURCES
Abraham Lincoln was a great president, but it wasn't just because he was a smart, thoughtful man. He surrounded himself with a cabinet comprised of his most bitter rivals, understanding the power of hearing from people other than "yes" men. Don't fall into the trap of listening to sycophants who tell you only what you want to hear. By seeking out contrary opinions, you'll avoid making decisions based on biased sources.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal*; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book* The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan*, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com.*

Start Planning Now!

Microsoft has announced Microsoft Windows 7 will no longer be supported as of January 14, 2020. This announcement gives you a little over a year to plan out your systems upgrade to Windows 10. If you are a current client, we will be assisting with the upgrade plan.

What are we reading: Cybersecurity for Executives

By Gregory and Joseph Touhill

To summarize, cybercrime affects all businesses large and small. With todays security risk, every business must have multiple layers of security protection.

The authors mention the deadly sins. Even though you think your business is protected, you remain vulnerable to human error. Hackers are professionals and have become an expert sending phony messages that look legit at first glance. I am quoting from the book, what are the deadly sins?

Ignorance—People may not know about cybersecurity risk and your rules and policies for reducing those risks. Remedy this with training. (If you are a TechSage clients, we offer online basic training. Please reach out to Beth to sign up your employees).

Apathy– Your staff members understand the risks and know your policies, but don't heed established security procedures. Warning signs include failure to complete security training and ignoring security rules. Does your company have security policies in place?

Stupidity—Smart people can do dumb things, as proven by an experiment conducted at a US government facility. Researchers placed thumb drives in the parking lot and waited to see what happened. People picked them up and inserted 60% of them into government computers, despite rules specifically barring such acts.

Curiosity—Phishing attaches prey on curiosity by, for instance, claiming to offer information about a fabricated problem with the recipient's bank account.

Lack of Leadership—Take cybersecurity seriously. If you're a top executive, you should attend training sessions. Be sure your people see cybersecurity as a grave issue.

Lack of accountability—Are your personnel ignoring security policies? If so, impose consequences. If you don't hold anyone accountable for missteps, risky behavior will continue.

Something we all should think about.

Refer a friend from now through September 30th, 2018 Get a $25 Gift Card & You'll Be Eligible to WIN a Apple Watch Series 3 (non cellular).

How the Contest Works:

1) Call or email us with your referral information and receive $25 gift card.
2) We will call your friend to schedule an appointment. If an appointment is made, we will send you a $50 gift card.
3) After the appointment we will add your name into the drawing for Apple Watch Series 3.
4) If your friend becomes a client and spends $1,000 or more, we'll send you a check for $100. As a bonus, we'll also give your friend a $100 discount off our services!

What makes a good referral for TechSage Solutions?

A business owner who has 5 or more PC's and needs help with their network, data backups, phones, email, data security, etc. or is just interested in having a second opinion on how they are doing things now. We provide service to the San Antonio area and surrounding cities.

Send email to info@techsagesolutions.com or call (210)-582-5814

Why is Advanced Endpoint Security Important?

There are some great anti-viruses on the market but do they totally protect you from Ramsomware and place offer a Ransomware warranty.

Being an IT Provider, we have seen a lot of cyber activity among small businesses. They are usually considered easy targets. This is why we are continuously looking for security tools to offer our clients.

SentinelOne Endpoint protects your computers and data from malware, viruses, and cyber attacks with advanced endpoint security. It is the only platform that defends every endpoint against every type of attack (executables, fileless, browser, scripts, etc.) at every stage in the threat lifecycle, pre-execution, on execution and post– execution.

SentinelOne offers a warranty to ensure that no ransomware attack will go undetected and cause irreparable change. The SentinelOne guarantees your protection against Ransomware attacks up to $1,000 USD per compromised endpoint, and up $1M per organization. Does your anti-virus has such a guarantee?

TechSage is using this as our endpoint protection and it has saved me personally several times.

Reach out to us if you would like more information:

Phone: 210-582-5818 or Email:

info@techsagesolutions.com