TechSage Solutions Newsletter June 2018

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:

3 Deadly Mistakes You're Making By Being Cheap

Today's small and midsize businesses (SMBs) have an uneasy relationship with technology – even if they don't realize it yet. As the marketplace reaches new heights of complexity and speed, and consumers migrate to cyberspace en masse to make their buying decisions, SMBs are responding in turn. Today's savvy business owners utilize ever-evolving technologies to capture their customers' interest and imagination, make conversions and manage their day-to-day operations with unprecedented ease and clarity. Certainly, the Internet age is a thrilling time to be in business. Each business is equipped with wildly powerful tech that has transformed the landscape of commerce forever.

But there's an uncomfortable truth that goes hand in hand with this increased dependence on technology. At its best, IT allows us to do incredible things we never would have imagined were possible even 10 years ago. At its worst, IT is an unreliable, finicky and potentially hazardous scaffolding upon which we built our loftiest hopes and dreams. Even the best IT requires wrangling to shape it to our needs and keep it on track and safe from intruders.

Despite this reliance on technology, the vast majority of business owners consider it an extra expense rather than a foundational element of their company. As a result, they skimp on technology spending. But being cheap comes with a cost – one much bigger and more dangerous than you probably realize. Here are three mistakes you're making by underspending on this key part of your business.

1. You're spending on technology based on an unrealistic, poorly planned budget rather than building your technology budget around your actual needs.

Continued on pg.2

Continued from pg.1

When you're an SMB with limited resources, it's easy to see any money saved on software and hardware as a success, leading businesses to opt for cheap, clunky and outdated solutions. But in a world where the lion's share of your day-to-day operations is dictated by the digital equipment you and your team use, where small businesses exist under constant threat of cyber-attack and data is a precious commodity that could disappear at the speed of a failed backup, cutting corners is unwise. Updating your digital approach and tightening your cyber security may not result in obvious, immediate returns on your investment. But adequate technology spending is just that – an investment. When you invest in the latest technology, you're investing in the long-term productivity and security of your business.

2. You're opening yourself up to disaster.

It's one thing to have an employee's computer unexpectedly fail or for an Internet connection to have a momentary hiccup. But if you're skimping on technology, you're leaving your business vulnerable to catastrophes that could cost you thousands. One of the most prominent and overlooked of these threats is cybercrime.

> **"When you invest in the latest technology, you're investing in the long-term *productivity* and *security* of your business."**

According to the 2016 State of Cyber Security in Small and Medium-Sized Businesses report, half of all U.S. small businesses fell victim to a cyber-attack in 2015 – a number that has only continued to climb. The majority of these attacks are ransomware, in which entire systems are locked out of vital data and forced to shell out enormous sums to recover it. Even if you assume you're secure (and you probably aren't), there are other risks to contend with. Server failures, backup loss and system downtime can shutter businesses just as easily as a vicious hacker.

3. You're letting the competition get ahead.

Outsmarting your competitors takes more than just mimicking whatever latest strategy the thought leaders of your industry are championing at the moment. It requires anticipating future trends and acting on them. And in business, there's one universal truth you can count on: The future of your industry lies in technology. Cloud services, new and constantly updating software, CRMs and a staggering array of productivity-enhancing tools are just a few of the advances your competitors are considering (if they haven't snatched them up already). If you neglect the future, your company is destined to become a thing of the past.

If you need assistance, please reach out to us by phone **210-582-5814** or email **info@techsagesolutions.com**

Free Cyber Security Assessment Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security assessment to uncover loopholes in your company's IT security.

After the assessment is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To Get Started And Claim Your Free Assessment Now –Call 210-582-5814

Shiny New Gadget Of The Month: Watch What You Ear With LinkSquare

Everywhere we go, most of us use vision to navigate our world. Whether our mouth begins to water at the sight of a tasty dish or our brow furrows at the sight of a shady looking dollar bill our eyes are one of our primary means of connection to the world around us. But, just by looking, can you tell whether that delicious looking food is as high quality as it seems? Or be absolutely sure that the dollar is real?

Enter LinkSquare, the pocket-sized spectrometer that enables us to gaze deeper into the objects around us. After you scan an object with the device, it uses machine learning to analyze the properties of all sorts of items, including the freshness of food, the authenticity of money or gold, the identification of stray medications and a hugh variety of other potential applications. If you're interested in purchasing this wildly futuristic technology, it'll cost about $300. Learn more at LinkSquare.lio.

Want A Stronger Team? Ask Better Questions

We'd be willing to bet that pretty much every leader is on the lookout for ways to run better meetings. It's a delicate balancing act to find the right combination of problem-solving, voicing concerns, and collaborating—and if you mess up that balance, you're unlikely to get anything done in a meeting at all.

One way to bring fresh energy to your next team gathering is to ask what two writers from leadership consultant company CVDL call "positive questions". These inquiries start from a positive aspect of your team or organization and use previous successes to spur your team to find a productive way toward. For example, a question like, "What are the factors that enable us to do our best work?" positions your team as the inciters of positive change, giving them an opportunity to think of real solutions that will drive everyone forward together.

3 Questions No Leader Should Ever Ask

At ghSMART, we advise board members and CEOs of large companies on their most important leadership issues. One of the most important skills we discuss is making sure they are consulting on the right questions.

I think of a "right" question as one that matters – a question that will cut to the heart of an issue, produce an answer on which the leader can act and provide the highest value to the leader in terms of results.

But the "right" question then becomes, "What are the wrong questions?"

There are three categories of "wrong" questions that I've heard time and time again over the years. Merely asking these questions can lead you down the wrong path when you're seeking to achieve your career's full potential.

1. If you have to ask an ethical question, just don't do the thing you were considering.

The wisest, most successful leaders I have served or worked alongside all seem to lead according to this rule regarding ethical questions: "If you have to ask, then don't." In other words, if there is something you're considering that's in a moral gray area or might be misinterpreted as unethical, then just don't do it. At ghSMART, we call this "having 110% integrity." We do things that are not only 100% ethical, but we give an extra 10% safety margin to avoid things that could be misinterpreted.

2. If you have to question whether someone is underperforming in their job, they are.

There's a common cycle of "facing reality" I often see my clients go through. They have a bold vision and a goal to achieve something great. And when they realize that they don't have the team to make it happen, they start totasty fantasize and think, "I wonder if Fred or Amy is going to rise to the occasion and display strengths we'venot yet seen to achieve these results." Great leaders know who they can count on. They don't expect a subordinate to suddenly start performing well in a role that does not appear to fit their talents and interests.

3. If you wonder whether you can trust your boss, you can't.

There is a saying: "People don't quit companies; they quit bad bosses." So if you find yourself wondering whether you can trust your boss or not, you likely can't. Instead, go find a boss you can trust. Find a boss who will hold your interests in high regard and care about your career goals as much as you do, giving you coaching and feedback to help accelerate your learning. These bosses will have your back during bonus time. Rarely do you see great leaders who wonder about the trustworthiness of their boss staying at that particular job very long.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times bestselling book, Who: A Method for Hiring, and the author of the No. 1 Wall Street Journal best-seller, Leadocracy: Hiring More Great Leaders (Like You) into Government. Geoff co-created the Topgrading brand of talent management. He is the Founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, an MA, and a PhD in Psychology from Claremont Graduate University.

What is your company's hiring process? To avoid hiring mistakes, I recommend reading and following Geoff Smart and Randy Street's book "Who". If you are familiar with "TopGrading", Geoff goes deeper with his dad's principles including generating a flow of A players, the right interview questions and process. You can find it on Amazon.com.

The Importance of The Company's Credentials

Password combination with your user id is only your entry into a website. When a company is hacked, it usually starts with obtaining usernames and passwords. Are your employees using multiple passwords for logging into software or websites or is it generally the same password? When cybercriminals find this information, they can use it multiple ways.

If an employee's credentials are compromised, cybercriminals can sell the information on the black market. As stated before, cybercrime is a very profitable business. This sold information allows a less than honorable person to login websites pretending to me you. If you use the same password across accounts, a cybercriminal cannot get to one website but many other websites. If you notice, many websites ask if you want to login using your Facebook or Google Gmail account. This is not recommended. A unique password should be used instead. There are several encrypted password vaults to store passwords. If one is used, a unique strong password should be used for creating your credentials.

Another recommendation is to use 2-factor authentication when possible. TechSage Solutions uses this tools for all of our company tools. Two-factor authentication identifies users by using a combination of two different components. If one of our employees' credentials are compromised, the cybercriminal can't proceed unless they can penetrate the next level. You probably noticed when logging into most banking institutions, they will either email code or send a text before you are allowed to completely login into your website destination. This is highly recommended for all business related websites.

Another tip is to set-up alerts on all financial sites. This has saved me several times from fraudulent charges.

Monitor the companies email accounts to identify any breaches. Any compromised employees email credentials should be addressed immediately.

Please contact us at **210-582-5814** if you need assistance.

Refer a friend from now through June 30th, 2018, Get $25 & You'll Be Eligible to WIN a Google Home.

How the Contest Works:

1) Call or email us with your referral information.
2) We will call your friend to schedule an appointment.
3) We'll send you (or your charity of choice) a check for $25 after the appointment and add your name into the drawing.
4) If your friend becomes a client and spends $1,000 or more, we'll send you (or your charity) a check for $75. 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 10 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 an email to info@techsagesolutions.com or call (210) 582-5814

Ten Ways To Stay Secure In The Social-Media World!

Social media allows millions of people to reconnect and stay up-to-date with family members, friends, acquaintances and even former in-laws. But as social media reshapes the way we communicate with one another, it's important to keep a couple of things in mind to protect yourself and your data.

Remember that there's no "delete' button on the Internet. Even if something seems temporary, a simple screenshot or check through the archives can make it permanent. Even if you keep your social media completely private, relationships change, and what was private yesterday may suddenly become public record. The question you need to ask is whether you'll be comfortable in 10 years with what you're posting today.

In the same vein, if you post in online forums or on message boards, consider using a pseudonym. Never share names or real businesses, clients, friends or family. If a bank manager wouldn't allow a picture of all the money in the vault to be shared on the web, you shouldn't allow a picture containing confidential, financial, legal or other protected documents and items to be shared either.

A good social-media policy in the office now can save headaches down the road.