



# 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:

This Is The #1 Security Threat To Your Business .....1&2

FREE Report: ..... 2

Shiny New Gadget Of The Month: .  
PetChatz HD Pawcall—FaceTime  
With Your Dog! ..... 3

4 Ways Smart People Blow The  
Close ..... 3

Start Planning for 2019 ..... 3

Geoff Smart ..... 3

What I Learned From Shark Tank  
Barbara Corcoran ..... 4

Top Tips You Can't Afford To Miss  
From A CEO Who Survived A  
Ransomware Attack ..... 4

Contest ..... 4



## This Is The #1 Security Threat To Your Business ... And It WILL Happen To You

Would you leave the front door of your business wide open every night? Of course you wouldn't. When nobody's at the office, you've got to protect your assets, usually behind locked doors, a complex security system and often even a network of CCTV cameras. There are procedures in place in case a thief ever wriggles their way into your facilities. And you've got insurance if the worst ever happens.

But what about your digital assets? According to a report from Kroll, digital theft of small businesses overtook physical theft in 2017, for the first time ever. As surprising as it may seem, today your business is more likely to be penetrated by hackers than from a disgruntled ex-employee to heist a few PCs in the dead of night.

Despite this, data shows that the vast majority of small businesses are seriously underprepared for cyber-attacks. The 2018 Verizon Data Breach Investigations Report states that a full 58% of malware strikes were on small businesses over the last 12 months, a number that continues to climb. The average cost of these attacks has climbed in turn, now exceeding \$1 million between efforts to recover data and restore daily business operations. Yet, according to a 2016 survey by the National Center for the Middle Market, less than half of midsize US businesses have an up-to-date strategy to address cyber security concerns and almost a third have no plan at all.

In effect, business owners are leaving their digital front doors unlocked, complete with a neon sign saying

*Continued on pg.2*



Continued from pg.1

While it's easy to assume you're safe from the kinds of large-scale digital breaches you read about in the news every week, that false sense of security will eventually come back to haunt you. With more than half of small businesses targeted for digital attacks every year, it's practically inevitable that you'll end up in the crosshairs of cybercriminals. Without the proper security measures in place, that \$1 million bill is going to hit your desk one day, and it may even shutter your business for good.

Luckily, with even a modicum of proper, proactive stewardship of your digital assets, you can turn that open door into a bank vault in no time. First, start with your employees. A full 51% of data breaches occur due to the negligence of hapless team members, according to CompTIA. Establish comprehensive security policies, lay them down in crystal-clear print and have your employees sign off on them. Build a thorough education program to school your employees on the risks and signs of digital crime. Topics should range from "How to spot a phishing e-mail" to the proper construction of company passwords.

While your employees are learning the ins and outs of

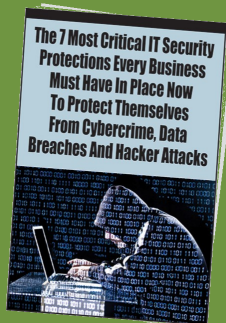


basic cyber security, invest in multilayered protections for your network. This must go beyond a simple, free antivirus, and should include platforms to keep all your patches up-to-date, security measures seamlessly integrated with company e-mail and, preferably, the watchful eye of a managed services provider. If you're not a professional, it's easy to miss security holes that would be glaring to criminals, even if you do your research. Better to get the experts involved and keep them patching those holes as they arise rather than risk missing something that flips your company belly-up down the road.

Thousands upon thousands of other small-business owners are leaving their digital door wide open day in, day out. As a result, cybercriminals have begun to consider companies like yours to be easy pickings, vulnerable fruit ripe for harvest. Don't be one of the millions of businesses that succumb to cyber-attacks every year. Invest in adequate protection and give yourself the peace of mind you need to focus on what you do best: making money.

**"In effect, business owners are leaving their digital front doors unlocked, complete with a neon sign saying, 'Rob me!' flickering above."**

### FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at  
[www.techsagesolutions.com/cybercrime/](http://www.techsagesolutions.com/cybercrime/)

© MARK ANDERSON

WWW.ANDERSTOONS.COM



"It's not a text abbreviation, it's a formula."



## Shiny New Gadget Of The Month:



### PetChatz HD Pawcall FaceTime With Your Dog!

When a product is advertised as “more than a pet-treat camera,” you know we are living in 2018. PetChatz HD PawCall is a two-way, interactive camera to connect you to your furry friends while you’re away from home. With a camera secured to the wall and a treat-motivated interface for dogs and cats to master, the device allows you to say a quick hello to your pets, see how they’re doing, and dispense treats or essential oils to calm them down and keep them happy. The device even lets you monitor your home for any intruders or problems that may arise during your pets’ home-alone time. A silent mode enables you to observe your pet in their natural habitat, while a two-way “chat” feature allows you to connect in real time. It’s the perfect gift for any pet enthusiast!

### Start Planning for 2019!



Microsoft announced that they are retiring the operating system Windows 7, and Windows Server 2008 which includes Small Business Server effective January 2020. What does this mean? When Microsoft retires an operating system, they are no longer perform security updates which leaves a hole in your network. As security vulnerabilities develop, patching is a must to keep your network secure.

Something to consider, there is a special tax deduction for small businesses titled “Section 179 election”. The Federal Government allows you to buy up to \$1,000,000 in 2018 in machinery, computers, software or tangible goods and **REDUCE** your taxable income on your current year’s tax return.

For further information, the website is <https://www.section179.org/>. I recommend consulting with your CPA for advice and further details.

# 4 Ways Smart People Blow The Close

*The weirdest thing happens when it's time to close a deal: smart people turn to mush!*

*I've seen it happen a hundred times. Even my own teammates, many of whom have PhDs and MBAs from some of the top universities in the world, aren't immune to this issue. When they're doing the work, my colleagues are confident, caring and even daring. But when selling the work, they often struggle. I see the same four fatal patterns with salespeople of all stripes.*

## 1 THEY HIT MUTE.

Recently, I was with a colleague in the boardroom of a billionaire CEO of the No. 1 company in his industry. This prospect actually said out loud that his No. 1 leadership problem is exactly what our firm is good at – hiring and leading talented teams across his portfolio of business. After he had outlined all the ways he wanted our help, the close should have been easy. But instead of sealing the deal, my colleague froze up and went silent. For an awkward 20 seconds, we sat there in silence. Eventually, we reached a happy conclusion, but in many cases, you won't be so lucky. Clients want help wrapping up a conversation and setting an action plan. Don't go quiet!

## 2 THEY AVOID “IMPOSING.”

After a long meeting, in which my colleague helped a high-powered CEO identify many of the key problems hindering his company, I watched in shock as he ended the meeting with no follow-up plan whatsoever. When I asked him why, he told me, “I didn't want to impose! I just felt like we were having such a good, trusted advising conversation, I didn't want to turn it into a sales call.” I asked him how helping a CEO solve his

No. 1 problem could ever be called imposing.

Think about it this way: It's one thing to help a leader identify an issue; it's another to help them actually solve it.

## 3 THEY DAZZLE WITH COMPLEXITY.

The urge to sound smart and impressive is a strong one, but don't let it get in the way of a sale. One colleague of mine explained our services to a prospect at 90 mph, throwing all kinds of compelling data points and analysis at him in a short span of time. But instead of being convinced by her breadth of knowledge, the prospect felt that he couldn't get a word in edgewise. Of course, it's vital that you know what you're talking about and you establish credibility with your prospects, but don't let that take priority over genuine communication and advisement.

## 4 THEY WIN THE ARGUMENT.

Clients are not often impressed with a confrontational “I'm right, you are wrong” posture. Folks, serving clients is not about winning arguments. Serving clients is about understanding them and figuring out how to get them what they want. You are on the same team. If you forget this, you may win the argument, but lose the deal.



Geoff Smart is chairman and founder of SMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling 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 Top grading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMART Kids 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, and an MA and PhD in Psychology from Claremont Graduate University.

All of us  
Join in wishing you a  
**HAPPY THANKSGIVING**  
And a wonderful Holiday Season!

## What I Learned From Shark Tank Barbara Corcoran

Barbara Corcoran, a Shark on Shark Tank ABC's hit reality TV show series spoke at our quarterly mastermind group this past October. She shared that she was a straight D student in high school and college and had many jobs until she met her future business partner when she was a waitress. This gentleman who became her boyfriend and business partner invested \$1,000 and gave Barbara an opportunity in real estate because he believed she could sale. The relationship dissolved which spurred Barbara to go out on her own.

Her company went approximately 18 years without a profit but Barbara was driven to succeed. She continued to money back into the business and taking risks. With all her trials she gradually built The Corcoran Group real estate company.



Out of the 70 companies she has invested in, 11 are very successful. She believes what contributes to their success is that they think fast on their feet and turn something bad into an opportunity.

Barbara loves to talk about sales, so she explained part of her success, she is always having conversations with people and recruiting where ever she goes. When she discovers someone that has a positive attitude and high energy level, they could be a potential team member. If she discovers talent, she will make room for them in her company.

She describes what does not make a good team member or sales person. This is generally the person that claims "it is not my fault", negativity, complainer or the blame game. These types of people do not last long in her company. She sets the expectation for her sales team if they don't sale something in 3 months, they can't continue with the company.

She was very funny explaining her childhood and her adventures through life. I recently purchased her book "Shark Tales" and anxious to read it.

**Refer a friend from now through December 31, 2018**  
**Get a \$25 Gift Card & You'll Be Eligible to WIN a**  
**Sonos-PLAY:3 Wireless Speaker for Streaming**  
**Music**

### 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 Sonos-PLAY3: Wireless Speaker for Streaming Music.
- 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](mailto:info@techsagesolutions.com) or call (210)-582-5814**

## Top Tips You Can't Afford To Miss From A CEO Who Survived A Ransomware Attack



Years ago, A1Care owner Percy Syddall upgraded his business with a state-of-the-art system for storing all the company's records and customer data in a single place. The network was a massive boon to both his customers and employees. But when his entire organization found themselves locked out of the data by ransomware, with the hackers demanding a price too steep to pay, the company had to act fast. They learned how to respond to an attack the hard way.

The first step was to evaluate the threat. They decided not to pay the ransom (which they couldn't afford, anyway) and instead thoroughly documented the issue. Then, they got the authorities involved and alerted their customers about the breach. In the end, the attack cost thousands of dollars, but they weren't about to let it happen to them again. They began looking for more powerful solutions that would prevent future attacks and started asking more pointed questions to determine exactly what vulnerabilities their system might have. Most importantly, they began to back up their files and trained their team to recognize threats before they became full-on crises. You live and learn.

SmallBizTrends.com, 7/14/2018

