RIGHT HAND TECHNOLOGY GROUP
TECH TIMES

November 2018

What's New?

See Something
Say Something!

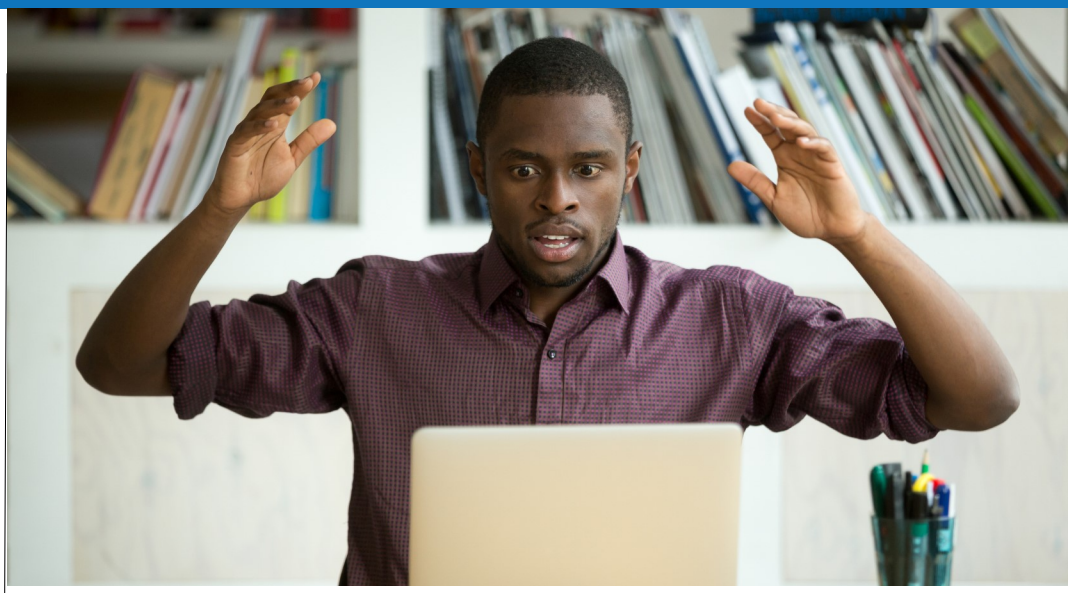
The most important security awareness rule you should follow: "See something? Say something." Or, "Report it now!" Or, "Report all potential security incidents IMMEDIATELY!"

Why the urgency? Why is IMMEDIATELY so necessary? Why can't you wait until after lunch to report an incident? Why should you choose to be three minutes late for a meeting just so you can report a security incident? Because resolution is all about time.

Think about it this way: You notice something a little odd, or different, or unusual, and think it should be reported. It could be in any of the Cyber, Physical, or People domains. From your view, the security incident is new, but you don't know how long it might have gone unnoticed. You don't know if it has caused any harm or not… because you just noticed it.

Now think: How much damage can a security incident cause in one minute? How much damage can that same security incident cause if left unreported for one hour? Is that 60 times the potential damage? Or what about one day, or even a week, or longer? You simply don't know; all the more reason to report any suspected security event as quickly as possible.

Time Is Not On Your Side The longer a security event goes unreported, the more potential there is for it to cause damage. Advanced Persistent Threats (APTs) often go unnoticed and unreported for more than a year. How much information can a criminal or hostile nation-state steal in a year? How much money might be lost? How much damage can be done? The answer? WAAAY too much...



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 for a disgruntled ex-employee to boost 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

continued on pg2

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 "Rob me!" flickering above. 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.

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

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.

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!

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 ghSMART. 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 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, and an MA and PhD in Psychology from Claremont Graduate University.

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

Years back, 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*

3 Ways The Digital Transformation Is Changing Our Everyday Lives

1. Artificial intelligence has gone mainstream. Amazon Echo, Siri, Google Home and other personal assistants would have seemed like science fiction even 10 years ago. But now they're just another facet of our contemporary reality.

2. Robots are continuing to push industry forward. You probably don't have an android making copies in your office, but"cobots"

(collaborative robots like Festo's BionicCobot) have started to intuitively automate manufacturing cycles and individualize even the assembly line.

3. Homes, cars and shopping are undergoing a revolution. Smart home platforms are becoming more and more common as we push forward, and those systems are becoming more and more advanced. Cars can drive themselves, to-do lists can order groceries without your input and digital technologies are leaking into every single aspect of our lives. *Inc.com, 1/22/2018*

Who Else Wants To Win A $25 Gift Card?

The answer to last month's Trivia Challenge Quiz was D) 1978

November's Trivia Question is Below:

You finish playing a game and remember you have that ten-page term paper to write before tomorrow morning. You breeze through it and now you need to spellcheck it. Which key can you press, on most PCs, for a spellcheck shortcut?

A) Tab

B) F12

C) Enter

D) F7

First Person To Email The Correct Answer to trivia@rhtg.net WINS!