BSSi2 Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

The Lighter Side….

A Sign in a Shoe Repair Store in Vancouver Read:
"We will heel you
We will save your sole
We will even dye for you."

At an Optometrist's Office:
"If you don't see what you're looking for, you've come to the right place."

On a Plumber's Truck:
"We repair what your husband fixed."

On an Electrician's Truck:
"Let us remove your shorts."

On Another Plumber's Truck:
"Don't sleep with a drip. Call your plumber."

At a Car Dealership :
"The best way to get back on your feet – miss a car payment."

Outside a Muffler Shop :
"No appointment necessary. We hear you coming."

In a Veterinarian's Waiting Room:
"Be back in 5 minutes.
Sit... Stay.."

At the Electric Company :
"We would be delighted if you send in your payment on time.
However, if you don't, YOU will be de-lighted."

In a Chicago Radiator Shop :
"Best place in town to take a leak."

On the Back of a Septic Tank Truck:
"Caution - this truck is full of Political Promises."

Your Cybersecurity Posture is Only as Strong as Its Weakest Link

From ProofPoint's 2020 User Risk Annual Report

Your cybersecurity posture is only as strong as its weakest link. And in today's people-centric threat landscape, that means your users. They are your greatest asset, your biggest risk and your last line of defense from threats. *(And you thought it was just BSSi2 with these opinions.)*

That's because attackers have shifted their focus from infrastructure to people. No matter how well you're managing your IT infrastructure, you can't patch your way out of these people-centered attacks.

Attackers' targets and methods are constantly evolving. Your Very Attacked People™ (VAPs)—those users facing the highest volume of attacks, the most advanced threats or most sophisticated tactics—aren't always your VIPs.

Many users do not apply key cybersecurity best practices:

- 45% admit to password reuse.
- More than 50% do not password-protect home Wi-Fi networks.
- 32% do not know what a virtual private network (VPN) is.
- 90% of working adults admit to using employer-issued devices for personal activities.
- Nearly 50% allow friends and family to access their work devices.

Users also need to recognize that **decisions they make outside of their inboxes** can put them (and your organization) at greater risk of phishing attacks and other threats. Smartphones and Wi-Fi are potential weak links. Nearly all survey respondents (95%) said they use a smartphone, and 41% said they use their devices for both personal and work activities. Here's how carefully they protect those devices.

Wi-Fi presents a challenge. Open-access networks are virtually everywhere, and device users readily connect (often to avoid data charges). Unfortunately, familiarity can lead to misplaced trust: 26% of global respondents think they can safely connect to public Wi-Fi networks in trusted locations, such as coffee shops and international airports.

Public hotspots aren't the only source of Wi-Fi danger. Working remotely has become more common, which means that home Wi-Fi hygiene can affect the security of your organization's data and systems.

ProofPoint found that 95% of global workers have a home Wi-Fi network. But are those networks adequately protected?

- 49% password-protect their network.
- 45% of respondents have personalized the name of their Wi-Fi network.
- 31% have changed the default password on their Wi-Fi router.
- 19% have checked and/or updated their Wi-Fi router's firmware.
- 14% are unsure of how to implement Wi-Fi security measures.

Continue on the next page...

... continued from the previous page.

- 11% said they find Wi-Fi security measures too time-consuming and/or inconvenient to implement.

When it comes to **end-user cybersecurity**, misconceptions are often at the root of risky behaviors. We found that many working adults mistakenly rely on technical safeguards on home and work devices to be failsafe solutions:

- 66% of survey respondents believe that keeping anti-virus software up to date will prevent attackers from accessing their devices.
- 51% think that their IT teams will be automatically notified if they accidentally install a virus or other malicious software on their work computer.

Passwords are another source of frustration for security and IT teams. Most concerning: users' tendency to reuse passwords. Password reuse, when part of a breach replay attack, is a frequent conduit of email account compromise (EAC) and cloud account compromise. Cyber criminals often use stolen passwords from one account on others, counting on some level of password reuse.

Work Devices: Those who have access to work data freely use their devices for personal activities. If your employees are not well versed in how to safely interact with email, websites and social media, their actions could lead to security risk. It's particularly worrisome to think of your employees' friends and family having access to your organization's PCs and smartphones. Though 51% of those with work-issued devices said they deny external access, plenty of people allow their loved ones—including children—to use their devices for a range of activities.

Employee Turnover: Most organizations deal with at least some employee turnover from year to year. That means they'll always have a mix of cyber-savvy and not-so-savvy employees. Younger workers don't always come armed with the cyber skills that are most important to your organization's mission and security posture. But at the same time, you shouldn't assume anyone is well informed if you haven't taken the time to assess their skill sets and close any knowledge gaps.

That's why you should incorporate **security awareness training** into your employee onboarding sessions. This move sets the tone that cybersecurity is important at all levels of the organization. **If you deprioritize best practices and cyber initiatives, so will your employees.**

Can I Get a Witness? Creating Better Client Stories

Here's the neuroscience. When we tell stories, they bypass the skeptical part of people's brains (their frontal cortex) and connect with their emotional brain (the limbic system). The good news is that this is where people make decisions.

When you break out those bullet points, the only two areas that light up in someone's brain are the ones that recognize language. Yup — these are in the frontal cortex, so you've just given them a reason to resist you.

Tell better stories. Here's one way to do that.

Have you ever asked people for a testimonial? Then followed up a million times to remind them? And when that small percentage actually responded, what did you get?

Dreck!

"Thank you, John, for the wonderful job you did. It was a pleasure to work with you, and I hope to get the chance to do it again."

Aarrrrrgh!

Stop Being Embarrassed

It was hard enough for you to ask in the first place, because you didn't want to look pushy or egotistical. Get over it! People who appreciate what you do usually are happy to recognize you.

But when you received the few sentences that said nothing, you thought you had no choice but to thank them and live with it. Try something better. Lead the process and make it easier for someone to give you what you want.

What's In a Good Story?

You avoid meaningless "happy-speak" when you ask specific questions: either in an email or a conversation:

1. What problem were you facing?

You probably already know this. But you're asking because you ultimately want to tell the story to attract other people with the same issue. This makes it good to start with the pain.

2. What were your concerns about working with me/my company?

I believe people should be skeptical about me and what I do — they're starting in resistance, after all. So I invite my clients to tell me about their fears. This ultimately shows the reader that these folks were no pushovers.

3. How did I work to solve your problem?

This is the crux. It will tell your reader — and you! — what makes you unique.

4. What results did you see?

Readers will want to know that you can move the needle for them. And if there are quantifiable outcomes, so much the better!

Making the Most of Your Story

You can stop here and have a good story. Or you can ask two more questions:

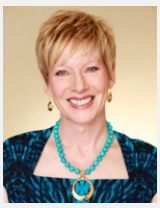
5. Under what circumstances would you recommend me/my company to someone else?

6. Is there anyone else you want to help to [name the problem you solved]?

Now you've turned a good story into a business development opportunity!

For years I've used this line about websites, but it's just as applicable here. "No one comes to your website to learn about you. They come to see themselves. And if you can show them you've already solved the same problem for someone else, you reduce their perceived risk in working with you — and shorten the amount of time it will take to contact you."

Create stories that *recognize* the people you work with — and *attract* the people you want to work with. Never again be satisfied with dreck!



Lynne Franklin works with CEOs of mid-size and large companies to break communication silos, create cultures where people want to work, and more easily meet financial goals. "Be a Mind Reader" TEDx Talk: http://bit.ly/2C9CE3G
lynne@lynnefranklin.com

Building Confidence as a Business Leader

How can you build your confidence as a CEO, investor or entrepreneur?

My colleagues and I at ghSMART see many talented people work hard to build their confidence.

New CEOs have imposter syndrome. Private equity investors who just raised another $1 billion in funds read newspaper headlines about the coming recession and quietly gulp. Self-made billionaire entrepreneurs worry that their fortunes will take an embarrassing hit. Newly elected government leaders worry about whether their results will live up to their campaign promises.

We find that leaders are less confident when they obsess about things they can't control, rather than take action in the areas they can control.

Like what?

The *Wall Street Journal* reported the results of a Conference Board survey (Jan. 16, 2019) of what is on the mind of 800 CEOs.

External Hot-Button Issues

1. Recession
2. Global trade
3. Politics

Internal Hot-Button Issues

1. Attracting and retaining top talent
2. Disruptive technologies
3. Developing the next generation of leaders

What this survey says to me is this: it's good to be aware of issues that are outside of your control – recession, global trade and politics. But it's even more brilliant to master the things that are within your control – hiring and retaining top talent, developing digital capabilities and developing the next generation of leaders.

How much confidence do you have in your team?

If you have a high degree of confidence in your team, then keep doing what you are doing to hire and develop them.

But if you don't have a high degree of confidence in your team, then you should focus on hiring, developing and retaining more of the right people who fit your strategy and who can achieve the results you seek.

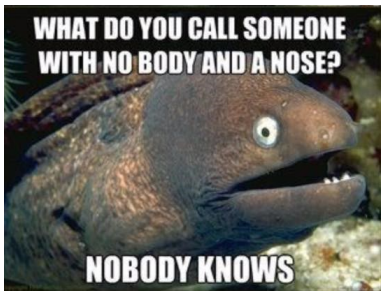
How?

There are three ways to build confidence in your team. You can invest the time to master the skills and best practices around hiring, developing and retaining top talent yourself. You can engage ghSMART to do it for you. Or (what most of our clients do) you can engage ghSMART to solve this problem immediately and build your skills in this area for your long-term success. (A quick side note: I'm very proud to report that my colleagues achieved 99% "high" client-reported satisfaction over the past 12 months. So, to go with this confidence theme, I have a very high degree of confidence that my team will help you solve your #1 problem!)

A great way to build confidence in yourself as a leader is to build your confidence in your team.

If you are the CEO of a company that generates over $1 billion in revenue (or has raised at least a $1 billion fund), then please reach out if you would like my team to help you build confidence in your team to deliver the results you want to achieve for customers, employees and shareholders.

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.



Business Tidbit

How Malware Can Cripple Your Business

Every year, the number of malware attacks on small businesses increases. Symantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people.

If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late.

~ Small Business Trends, Oct. 12, 2019

July 2020

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Shiny New Gadget of the Month

FitTrack

A Smart Scale That Does More

The bathroom scale isn't always the most useful device in the home. FitTrack is a smart scale that aims to change that. It's a different kind of bathroom scale that gives you much more than a single number.

Traditional bathroom scales don't tell you anything about what's happening in your body. FitTrack does. It gives you an "inside look" into what's going on inside your body. It measures your weight, body fat percentage, body mass index, muscle and bone mass, hydration and more. In fact, it tracks 17 key health insights.

The advanced scale pairs with the FitTrack app, which you can download to your smart phone and connect to the smart scale. All you do is step on the scale with your bare feet – the scale actually reads electrical signals from your body – and it sends the results to your phone. Simple and useful. Learn more about FitTrack at bit.ly/2VOg7Vs.

Stay up-to-date

Follow BSSi2 at:

www.facebook.com/bssi2

twitter.com/BSSi2llc

The Pets of BSSi2

Meet Hope, Simon's pup:
She is a sweet 80lb, 2 year old girl.