WCI Technology Insider

Insider Tech Tips - Written for Humans, Not Geeks

## *The Challenger Customer:*

### *Selling To The Hidden Influencer Who Can Multiply Your Results*

By Brent Adamson

We all love the customers who are ready to buy right away, but they're not always the *best* customers. In truth, it's the holdout that can really be your perfect customer. Authors Brent Adamson, Matthew Dixon, Pat Spenner and Nick Toman take this idea and run with it in their book *The Challenger Customer: Selling To The Hidden Influencer Who Can Multiply Your Results*. All four writers have been on the front lines of sales and marketing. They know how to turn a seemingly cold customer into someone who can very well lead to lasting results. If you're ready to shift your business into growth mode, this book is a must-read.


**November 2020**

**Bill Wright**
**Founder & CEO**

Our Mission:
Technology systems that anchor your business and protect what you have built, from a company inspired to make the world better.

# 4 Questions your IT services company should be able to say "yes" to

Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

*Continued on Page 2 ...*

*... Continued from Cover*

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT services partner – if you have a partner – and tell them you need help. They might be able to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position.

And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!"

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to.

1. **Can you monitor our network and devices for threats 24/7?**
2. **Can you access my network remotely to provide on-the-spot IT support to my team?**
3. **Can you make sure all our data is backed up AND secure?**
4. **Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?**

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

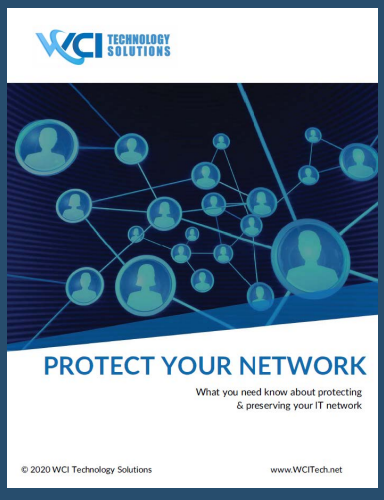
Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

## FREE Report: Protect Your Network

**You will learn:**

- The only way to know for SURE your data can be recovered if lost, corrupted, or deleted – yet fewer than 10% of businesses have this in place
- Seven things you should absolutely demand from any off-site backup service
- Where many backups fail and give you a false sense of security
- The #1 cause of data loss that businesses don't even think about until their data is erased




**Claim your FREE copy today at www.wcitech.net/protect-your-network**

## Microsoft 365 Tip

If you love Microsoft Teams but hate the notifications, they're really easy to customize.

Look at the top of Teams, over in the top right corner. Click on your profile picture, then select the Notifications tab.

Now you can set the alert type and frequency that best suits you.

# Is there a *secret intruder* hidden in your business?

**You might think that hackers won't target your business. But actually, you'd be surprised. Cyber criminals are targeting businesses exactly like yours all the time.**

Because often, small and medium sized businesses don't spend big bucks on their cyber security. Hackers know this. And they'll put a lot of effort in to trying to exploit that.

We're seeing a rise in ransomware attacks. This is the computer attack where a hacker locks you out of your systems and data. And you must pay a ransom, typically in Bitcoin, to get access again.

While it's not a new crime, it's one the fastest growing crimes online.

Reality check: This kind of attack can cripple your business.

**Hackers will encrypt or delete all of your data, leaving you to:**

- explain the breach to your clients
- try to restore what you've lost (that's if you have a working backup saved off-site that hasn't been affected) and clean up your network
- Or just pay the large ransom to undo the damage

It can cost thousands. And accounts for a scary number of businesses going under.

But if you know the warning signs to look out for, you can dramatically reduce your risk of falling victim to a hidden hacker that's already in your system.

**Can we offer your business a breach detection review?**

During the review, our specialists can carry out a detailed network check to detect if there has been any unauthorized activity. And give you advice for preventing this kind of attack in the future.

*Before we carry out the review, we'll need to have a quick video call (no more than 15 minutes, we promise) to discuss your current security, your business, and to answer any questions you may have.*

**Visit //www.scheduleyou.in/53PTQqp to book your call**

## SHINY NEW GADGET OF THE MONTH
## Arlo Pro 3 Floodlight Camera

In the era of porch pirates, more people are investing in outdoor security cameras. The Arlo Pro 3 Floodlight Camera delivers security and practicality. It features an ultrahigh-definition camera delivering 2K HDR video and color night vision combined with a 2000 lumens light. Nothing goes undetected!

Plus, the Arlo Pro 3 is wireless. It connects to WiFi and doesn't need a power cord (it just needs to be plugged in for charging periodically). Because it's on WiFi, you can check the feed anytime from your smartphone. You can even customize notifications so you're alerted when it detects a car or person. And it has a speaker and microphone so that you can see and talk to anyone near the camera. Learn more at **Arlo.com/en-us/products/arlo-pro-3-floodlight.aspx**

## De-clutter Your E-Mail Inbox in 2 Steps

1) Use the unsubscribe button. Look at how many e-mails you actually read from senders outside of your organization. Do you have a ton of marketing mail, promotions or newsletter you don't read anymore?Start hitting unsubscribe and leave behind only those message that you care about. Suddenly, you'll start receiving fewer e-mails every day.

2) Filter everything. Most e-mail clients allow you to filter by source or sender. Create filters that auto-sort e-mails into specific folders. That way, internal memos go to one folder, client messages to another, newsletters to another still and so on.
While filtering e-mails can be time-consuming, it's definitely worth your time.

# 4 Steps to move your business from defense to offense *during times of disruption*

*"Everyone has a plan until they get punched in the mouth." –Mike Tyson*

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant.

You have two options:

1. Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let's face it, that's not happening).

2. Create and act upon a new game plan. One that's built to overcome disruption and transform your business into something better and stronger.

Option Two is the correct answer! AND, we at Petra Coach can help.

At Petra Coach, we help companies across the globe create and execute plans to propel their teams and businesses forward. When disruption hit, we created a new system of planning that focuses on identifying your business's short-term strengths, weaknesses, opportunities and threats and then creates an actionable 30-, 60- and 90-day plan around those findings.

**It's our DSRO pivot planning process.** DSRO stands for Defense, Stabilize, Reset and Offense. It's a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn — better and stronger than before.

**Here's a shallow dive into what it looks like.**
**Defense:** A powerful offensive strategy that hinges on a strong defense. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

**Stabilize:** The secret to stabilization is relentless communication with everyone.
That includes internally with your teams AND externally with your customers. Streamline communication and eliminate bottlenecks through a visual dashboard.

**Reset:** By completing the first two steps, you'll gain the freedom to re-prioritize and focus your efforts on the most viable opportunities for growth.

**Offense:** Don't leave your cards in the hands of fate. Shifting to offense mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

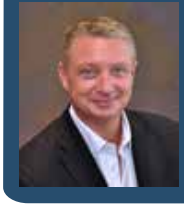
Interested in a deep dive where a certified business coach will take you (and up to three members from your team) through this process? Attend Petra's DSRO pivot planning half-day virtual group workshop. (We've never offered this format to non-members. During this disruptive time, we've opened up our coaching sessions to the public. Don't miss out!)

When you call a time-out and take in this session, you'll leave with:

- An actionable game plan for the next 30, 60 and 90 days with associated and assigned KPIs
- Effective meeting rhythms that will ensure alignment and accountability
- Essential and tested communication protocols to ensure your plan is acted upon

I'll leave you with this statement from top leadership thinker John C. Maxwell. It's a quote that always rings true but is crystal clear in today's landscape: "Change is inevitable. Growth is optional."

Let that sink in.



*Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.*

## Tech Fact#1

**Google rents goats – yes, goats – from a company in California, to help keep weeds under control at its HQ**

## Tech Fact#2

**You know that Bill Gates got rich from making Windows for PCs. But did you know his architect designed his house on... a Mac!**

## Tech Fact#3

**In an average day in the office, your fingers travel the equivalent of 12 miles over the keyboard**

## Tech Fact#4

**GPS is free for us to use all day, every day... but it costs $2m a day to run. Taxpayers like you and me foot the bill**

# TECHNOLOGY UPDATE

### I hope your family and business haven't been too badly affected by Covid.

Most of us have adapted to it now, haven't we? And I think we've accepted that nothing's going back to how it used to be for a long time.

There have been a lot of positives from this year. Lots of us have changed our lifestyle habits; spent more time with our families and got outdoors more.

We're certainly seeing technology benefits for lots of the businesses we look after. Some have now fully embraced the cloud, as the answer to any person working anywhere, on any device.

Others say they can sleep better because they now have robust data security in place (essential for remote working).

**What are the technology benefits your business has seen this year? Not sure where to start? That's OK, we can help you.**

Give us a call at 614-763-2911 and we'll guide you through the process

WCI TECHNOLOGY SOLUTIONS

## Inspirational Quote of the Month:

***"Technology is best when it brings people together."***

**- Matt Mullenweg creator of WordPress**

# When did you last check your backup?

**If you're taking data seriously in your business, you'll have a robust constant backup process that stores multiple copies of all your data safely and securely in the cloud.**

This can be a life saver in many situations:

- If your data is corrupted
- If someone accidentally deletes something
- Or even if you lose a device

But when did you last check that your backup was actually working? That it's correctly backing up your data exactly as it should be?

You'd be surprised how often backups fall over... and no one is alerted. Or they are alerted, but they don't take action to fix the problem fast enough.

This is why we verify our clients' backups on a daily basis.

If you haven't checked your backups for a week or more, then you could be setting yourself up for a big problem.

Because the worst time to find out that your backup hasn't been working is when you actually need it. And we've heard of this happening more than a few times.

Very easily, a business can lose a week or month's worth of work... it's a genuinely traumatic event.

So check your backup today to keep yourself covered.

*or if you'd like that taken care of for you, we'd love to help. Give us a call to see how we can give you one less thing to worry about.*

## Come hang with us on social media!

@WCITech

WCI Technology Solutions

@WCITech

## LATEST TECH ALERT

### Fancy a flip phone again?

**Do you remember flip phones back in the 00s? Well – they're back, but this time you can flip your smartphone.**

It's hard to believe until you see it – but the Samsung Galaxy Z Flip has a foldable screen. Yes, the glass actually folds. It runs Android and will set you back about $1,299.

# Are you forgetting something?

**Don't worry, you haven't missed our birthday**

We're talking about your office printer. When was the last time you thought about it (and we don't mean those angry thoughts when it starts scrunching up paper)?

We mean thinking about it from a data security point of view. That big hunk of plastic and metal needs attention. Because it's on your network. And it probably has an internal memory of all the documents that have been sent to print.

That means it's a threat when it comes to data theft.

Make sure your printer is password protected. That it's secured and accessible only by relevant people. And that old printers have their memories wiped and are correctly disposed of.

## Need a hand?

We can help you. Give us a call at 614-763-2911 and we'll make sure your entire network is secure and protected.

## Let's chat

### Three questions for you:

1. Do you currently have an IT support company?
2. How happy are you with them?
3. If the answer isn't "they're amazing", let's jump on a Zoom

**Covid has taught businesses round here just how important proactive, responsive IT support is.**

**We're now taking on new clients again.**

If you'd like to set up a 15 minute Zoom, go to my live calendar at

**https://www.scheduleyou.in/53PTQqp**

### QUESTION

**What software should I use for video calls?**

### ANSWER

Zoom is popular, and Microsoft Teams. It's really down to personal preference. Start by looking at how often you'll be making video calls, and with how many people. Then you should try 2 or 3 different apps to see which you prefer.

### QUESTION

**Do I need an external mic and web cam?**

### ANSWER

These can certainly add a professional polish to your video calls. But most modern laptops have perfectly good built-in microphones and web cams, designed for exactly this kind of communication.

### QUESTION

**How do I switch off when I'm working from home?**

### ANSWER

We've found it useful to have a dedicated work area, and only work there. If you don't have a home office, even a specific chair at a table that's only for work can help you mentally switch between working and resting.

Bill Wright, Founder & Chief Visionary Officer

1989

> GOOD LEADERSHIP IS MAKING THE CHOICE THAT IS BEST FOR THE WHOLE TEAM, NOT JUST THE LEADER, EVEN WHEN IT'S INCREDIBLY DIFFICULT.

2020


WCI TECHNOLOGY SOLUTIONS

81 Mill Street, Suite 300
Gahanna, OH 43230

@WCITech

WCI Technology Solutions

@WCITech


# Is working from an office more secure than working remotely?

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office. *If* done right.

Those are the three operating words: *if done right.* This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

**Secure networks.** This is nonnegotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

**Secure devices.** All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use employee-provided or approved devices for work-related activity.

**Secure passwords.** If employees need to log into employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board. *Entrepreneur, June 17, 2020*

**TOP TIPS ON HOW TO PREVENT YOUR SMART CAMERAS FROM BEING HACKED**

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

**1. Regularly update your passwords.** Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

**2. Say no to sharing.** Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

**3. Connect the camera to a SECURE network.** Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. *Digital Trends, May 7, 2020*