IT Times

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

This monthly publication provided courtesy of Brian Bratchie, president of B&L PC Solutions, Inc.

Our Mission:
We take care of technology so you can take care of business.

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 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

> **"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!"**

of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

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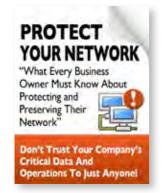
If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

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: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.BLPC.com/protect

Cartoon Of The Month

"Before we reposition ourselves as an industry leader, how was everyone's weekend? Anyone do anything fun?"

Declutter 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 newsletters you don't read anymore?

Start hitting unsubscribe and leave behind only those messages 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.

Genes And Greenhouses

Dandelions are very resilient. They can thrive in almost any condition. If your genes are like a dandelion's, you'll be able to adapt to difficult circumstances and overcome obstacles.

Orchids, however, are not resilient. They require very specific conditions to thrive. If your genes are like an orchid's, you have a greater risk of failure when facing harsh conditions.

If you had a choice, would you want to be like an orchid or a dandelion? Which would you want your children, students, or employees to be like?

Conventional perspectives emphasize the value of adaptability and flexibility – dandelion-like genes.

Orchid-like genes are traditionally seen as a liability. According to an article by David Dobbs in *The Atlantic* that explores recent genetic research, these genes increase the likelihood of "depression, anxiety, attention-deficit hyperactivity disorder, heightened risk-taking, and antisocial, sociopathic, or violent behaviors, and other problems." Doesn't sound too good, does it? But this isn't the whole story.

This genetic vulnerability is activated by negative experiences, especially early in life. Childhood trauma seems to trigger the negative potential of these orchid-like genes. Children who don't go through traumatic events don't experience the downside of their fragile genes.

Additionally, Dobbs writes that scientists are now realizing "**these bad genes** can create dysfunction in unfavorable contexts, but they can also **enhance function in favorable contexts**." People with orchid genes aren't just vulnerable to bad experiences; they are more sensitive to all experiences.

Unfortunately, "most work in behavioral genetics has been done by mental illness researchers who focus on vulnerability. **They don't see the upside because they don't look for it**," according to Dobbs.

What we are learning is that orchids "wilt if ignored or maltreated but **bloom spectacularly with greenhouse care**." Studies show that when people with supposedly bad genes "are put in the right setting, they don't merely do better than before, they do the best," even better than their peers.

This research confirms my belief that characteristics perceived as weaknesses in one situation are actually powerful strengths in another. The situation is very influential. We don't find success by eliminating our weaknesses and becoming perfect, but by finding the right fit. And sometimes **we need others to help us find or create the right environments**.

This is important for our relationships with our children, students, spouses, coworkers, employees and friends. It is tempting to emphasize weaknesses and dismiss people who aren't as hardy, resilient or flexible as others. However, in doing so, we might lose the people who have the most potential. **Our job is to create environments that allow orchids to bloom**.

Remember, in the real world, we see dandelions as a nuisance but we prize orchids for their rare beauty. Maybe we need to start doing the same in our lives.

David Rendall is a prominent keynote speaker and author of several books, including The Four Factors of Effective Leadership *and* The Freak Factor. *He holds a doctor of management degree in organizational leadership and a graduate degree in psychology. Prior to becoming a speaker, he was a leadership professor, stand-up comedian and nonprofit executive. As a speaker, his clients have included the U.S. Air Force, Australian Government, and Fortune 50 companies such as Microsoft, AT&T, UnitedHealth Group, Fannie Mae, and State Farm. Learn more about David at his website, DRendall.com.*

Inside This Issue

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 employer-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*