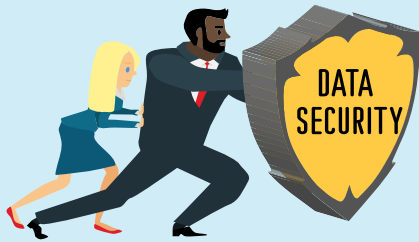## Make Your Employees the Frontline of Cyber Defense

DATA SECURITY

Cyber-attacks are becoming all too common. Because employees are the core of any business, they're typically the main target for cyber criminals. Making sure your people stay up-to-date with cyber security knowledge, and teaching them to recognize threats, is imperative.

An effective, ongoing internal security awareness program can help reduce your company's vulnerability, turning the "weakest link" in your cyber defenses into its greatest strength.

Security awareness training and phishing simulations can test employees on how they would respond to a real-life phishing attack.

Reduce business risk today by adding phishing simulations and security awareness training as another layer of protection from the ever-growing and evolving cyber threat landscape. Call now to get started: (512) 388-5559

This monthly publication provided courtesy of CTTS, Inc.

The #1 Mistake Your Employees Are Making Today That Lets Cybercriminals Into Your Network

In the wake of unprecedented rates of digital crime and the cost / frequency of data breaches constantly skyrocketing year after year, companies all over the world have been forced to scramble for solutions. There's an arms race running behind the scenes of every piece of technology we use in business today, as cyber security companies shore up their clients' defenses against increasingly sophisticated digital threats.

Billions of dollars are now poured into batting away would-be intruders from the most precious assets on global networks. Most of the money is directed toward the software that keeps everything afloat, just out of reach of the bad guys.

Even as each day brings a new technological apex for security solutions, data breaches continue. Despite the fact that the tools hackers use to make money are more or less the same as they were three years ago, nobody seems to question why companies are still being hacked at record levels. It's easy to imagine a crack team of infamous hackers hammering away at a keyboard into the late hours of the night, feverishly computing the one piece of code that will break them into a system.

This may be the process behind the high-profile breaches you read about in the news each week, but in reality, most cybercrime takes much less effort. The average hack succeeds not because of overt vulnerabilities in the structure of business networks, but because of a mistake made by you or your employees. According to IBM's

X-Force Threat Intelligence Index, more than two-thirds of breaches arise from what they call "inadvertent insiders," folks who accidentally left the network vulnerable from one action or another without even realizing it.

Most of the human error that becomes the root cause of catastrophe can be traced back to phishing. A criminal spends some time researching your organization, maybe learning a bit about an employee or two, and decides to masquerade as someone worthy of trust either within your team or from a company you contract with, or just a stock person offering something pretty much everybody wants. They mock up a somewhat convincing email and send it off to 10 people within your business. Somebody clicks the included link without thinking, and there you go – you've got ransomware. If you haven't backed up your data, you're looking at a hefty fee to get everything back, if they even give it back at all.

> **"Somebody clicks the included link without thinking, and there you go — you've got ransomware."**

In other cases, your team may actively duck around your previously implemented security measures or avoid the procedures you've put in place to keep the business safe. That can mean visiting unsavory websites, ignoring a vital security patch or another minor transgression. But when every mistake spells a potentially massive

vulnerability, you can't afford people who aren't conducting business to the highest standards in cyber security.

Regardless of how it happens, most hacks occur because employees just don't know better. Even in 2019, when cybercrime runs rampant and virtually everyone is constantly at risk on the Internet, most of us just aren't well-versed in ways to protect ourselves, much less the companies we work for.

The good news is that this problem is pretty easy to prevent through education. To keep everyone abreast of the latest threats to their livelihood, it takes a thorough set of rules, guidelines and general savvy to steer them through the troubled waters of modern cyberspace.

Of course, this will take more than a 30-minute crash course in the break room one afternoon. It'll take a concerted effort and dedicated resources. Luckily, we can help. With a trusted partner dedicated not only to keeping your organization protected from the latest digital threats, but to keeping your employees alert and ready to spot anything phishy, you drastically decrease the chances of your business becoming another statistic in the war on cybercrime. Work with us and secure the future of your company for the long haul.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eyeopener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call our office at:
(512) 388-5559

Luck Is NOT A Good Strategy When It Comes To Your Company's Data!

What would you do if a major virus or hacker attack destroyed your data? What if a natural disaster, fire, or flood wiped out your server…or if a hard drive failure or software malfunction corrupted your entire data system?

Some business owners are literally walking on a tight rope without a net, and don't realize it until it's too late.

That's why thousands of businesses lose millions of dollars worth of data to disasters like fires, power outages, theft, equipment failure, and even simple human mistake.

Fortunately, there is a way to positively guarantee your data can be restored quickly and easily. With our proven "Autotask Endpoint Protection (AEP)" you can rest assured your data is being backed up in a format that is not only secure, but also easily recovered when you need it.

With CTTS AEP:

- Your files are automatically backed up every night.
- Your data is safe from fire, floods, storms, viruses, hackers, hardware malfunctions, and human error!
- Should a disaster occur, you can be back up and running the very next day.

Call us today to learn more: (512) 388-5559

The Self-Made Myth: All Business Leaders Had Help Along The Way

I'm about to share an unpopular opinion: the self-made CEO is a myth. No successful entrepreneur or business leader is a self-made man or woman. If you think you are, you need to take a long, hard look in the mirror. Behind your successes are countless contributions from family, friends, teachers, mentors and coaches. If you can't see that, you're not looking hard enough.

As a business coach, I've seen companies grow from kitchen tables to $100 million enterprises and then collapse because the owners thought they knew everything. In contrast, the world's most effective leaders know they didn't get to where they are by themselves. They recognize that ideas can come from anywhere, and they actively seek out people who can help them on their journey.

Here Are Three Ways To Harness That Inspiration:

1 Rely On Your Team, And Show Your Appreciation.
The most effective leaders are always the first to admit that they don't have all the answers. They ask themselves tough questions to understand their own strengths and weaknesses, and they don't let ego or pride get in the way of building their companies.

One of the biggest mistakes I see business leaders make is thinking they can't learn anything from the people around them. It's essential to recognize your limits, seek others' help and opinion to patch holes in your expertise and give credit where credit is due.

2 Rip Off And Duplicate – The Other R&D.
Some of the best ideas I've had for my businesses are ones I've borrowed (and modified) from others. In my experience as an entrepreneur and coach, I've seen firsthand how ideas that are considered standard practice in one industry can be innovative when applied to another. Of course, it's about how you adapt those ideas to your business, not necessarily just copying what your competitors are doing. Instead, use the existing base of knowledge to provide a novel solution.

3 Crowdsource Ideas From Fellow Business Leaders.
Finding new solutions to business challenges is a never-ending and often exhausting task for entrepreneurs and business leaders. One source that I've used to help me solve problems has been a business advisory group (BAG) comprised of professionals in business operating in noncompetitive markets. Peers in a BAG can relate to the daily challenges you face running your company, managing teams and growing the business. BAG members can provide you with valuable insight into how they are running their own companies and how business solutions they've implemented may apply to your business.

Business is a team sport. No great company has ever been built solely atop the efforts of a single person. The entrepreneurial spirit will take you far, but eventually, you have to recognize that you need to rely on the ideas and contributions of others. When that happens, you'll become a greater leader, and you'll see your business and company culture grow exponentially.

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.

3 Ways To Make Your Customers Love You

With so much emphasis placed on finding customers today, business owners often lose sight of keeping the ones they have.

Here are 3 ways to win the devotion that makes for loyal customers:

1. Be Available.

Today, when customers expect products to be available on-the-go, businesses must do the same. Set up reliable resources to update and manage customer experience. For example, by setting up an automatic callback system, instead of waiting on hold, callers get added to a list then receive the call when the service team is ready. Live chat, an informative online FAQ and other handy resources can go a long way toward avoiding frustration.

2. Surprise Customers By Actually Being Convenient.

We've all had interactions with customer service that made us want to pull our hair out. Avoid this by reducing friction wherever possible. Make sure the people in charge of customer experience, whether it's a front-desk person or a team of dedicated service professionals, are friendly and transparent about the service process. Make signing up for appointments abundantly easy and pleasant, and you'll see the benefits in no time.

3. Put Your Money Into The Most Important Investment.

We all know that acquiring new customers costs seven times more than keeping existing ones. That makes the numbers pretty clear: you need to invest in your existing customers or risk going under.
Inc.com, October 4, 2018
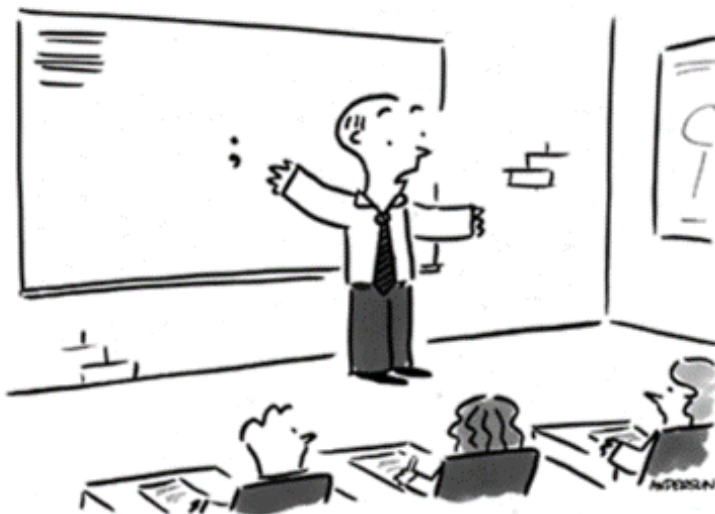
Can You Afford To Lose $80,000 A Year?

If Not, Read This:

According to the Better Business Bureau's 2017 State of Cybersecurity Among Small Businesses In North America report, SMBS lost more than $79,000 to cybercriminals. Honestly, this shouldn't surprise anyone; after all, as even the smallest businesses digitize more and more of their processes, the costs of breaking those systems will continue to skyrocket. If you're a small business owner in 2019, you need to start making cyber security a priority – now. Make a list of clear goals and objectives, and prepare your business for threats coming from all directions, rather than relying on a single defensive strategy that's prone to fail when things get tough.
SmallBizTrends.com, 12/3/2018

© MARK ANDERSON   WWW.ANDERTOONS.COM

"Can anyone, *anyone*, tell me how a semicolon is used other than in emoticons?!"

Get More Free Tips, Tools and Services At Our Web Site: www.CTTSonline.com
(512) 388-5559