Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
March 2018

# Please Welcome Michelle Quick!

We are excited to announce, we have a new Team member! Meet Michelle Quick! Michelle is our new Administrative Assistant and will be providing our Clients the prompt, courteous, and professional reliability they've come to depend on from CTTS.

Michelle attended North Carolina State University and recently worked as a Customer Service Supervisor at ADAO Global as well as helped out with general office assistance after being a stay-at-home mom for 12 years.

Prior to that, Michelle was an Executive Assistant at an Architectural firm. At the architectural firm she handled contracts, marketing, office management, clients, and assisted the Accounting Department.

At CTTS, she will be answering the phones and assisting the Accounting and Sales departments. She is a welcome addition to the CTTS Team!

Next time you call in, be sure to welcome Michelle!

This monthly publication provided courtesy of CTTS, Inc.

# 5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the Harvard Business Review – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

**1 They'll slip up because they don't know any better.**

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not

only leaves them vulnerable, but it leaves your company vulnerable as well. For this reason, most cyber-attacks come down to a lack of cyber security education.

**2 They'll let you get hacked on purpose.**
It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

> **"It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data... [b]ut there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people."**

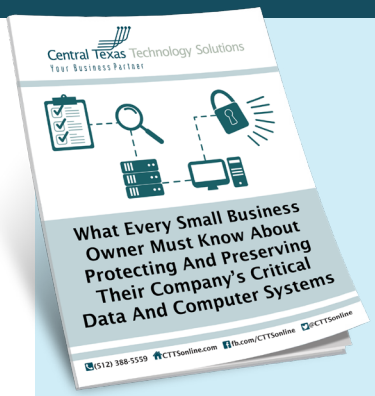
**3 They'll trust the wrong person.**
For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

**4 They'll miss red flags while surfing the web.**
Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

**5 They're terrible at passwords.**
According to Entreprenuer.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

## **Free Report Download:** 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 common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.**

**Claim Your FREE Copy Today at [www.CTTSonline.com/Protect](www.CTTSonline.com/Protect)**

# Back it Up Right

In today's business world, having a reliable way to access your data is key to your company's success. Everything you do hinges on the data you have at your disposal--so what would you do if that data was no longer available to you?

This is a far too common circumstance that creates problems for many businesses. It doesn't help matters that so many factors can lead to data loss.

Malicious programs, hardware failure, even a "whoops" moment from a user, can put your data in peril.

Even worse, events like these have a way of causing businesses to fail, as they no longer have the tools they need for success. However, there are methods to protecting your business from these issues.

One such method is to maintain a comprehensive backup to ensure that, regardless of what may happen, your critical data will be safe. With a solution that takes a snapshot of your data every 15 minutes, you can keep your losses to a minimum should something go down.

In case you didn't know, March 31st is World Backup Day. At CTTS, we dedicate a lot of time and effort to implementing and managing comprehensive data backup and disaster recovery solutions for Central Texas businesses. To that end, we have the solution your business needs to protect and preserve your information, and we can equip you with a backup plan that specializes in your company's unique data needs.

CTTS has the experience you'll want in a provider of such an important consideration. Give us a call today to hear how we can defend your data: (512) 388-5559

# The Top 3 Things I have Learned From Captain David Marquet

I recently had the privilege to meet Captain David Marquet and hear him speak on his experiences as a commander in the US Navy. After taking on the USS Santa Fe, the worst performing submarine in the fleet he was able to turn things around and build one of the best team environments in the Navy, which inspired his latest book, "Turn the Ship Around."

I'd like to share with you the top 3 things I learned from Captain Marquet:

**1 Leadership is a Language**
When Captain Marquet noticed his crew continually passing the blame on others, he made a rule, "No 'They' on Santa Fe." Although difficult at first, when crewmates began to say "we" instead of "they", there was a change in the way of thinking which allowed for ultimate team building. Captain Marquet says we need to "act our way to new thinking" and by practicing this change in wording, the change in behavior eventually fell into place.

**2 Don't Delegate, Elevate**
Although it may seem easier to order your employees to complete their tasks a certain way, wouldn't it actually be more efficient to not waste your time telling them to what to do? When you give your Team the information they need for success and let them have the freedom to decide how to accomplish their tasks, you are empowering them to have a sense of ownership over their job, which can only improve their performance.

**3 Give Up Control**
By making the work environment a place that embraces variability, you are creating a safe place for growth. You are not the only one who has to keep your company in check. Your Team should feel comfortable enough to voice their opinions and concerns. Listening to your employees will only strengthen your relationships and create a dynamic workplace. There are many things in this life that we cannot control, but when you learn to loosen the reins and let go a bit, you'll find an authentic willingness that allows creativity and competence to flourish.

# Want to take home this YETI Cooler?


Refer us to the CEO/Owner of another business in the Central Texas area, and for each business you refer to CTTS we will put your name in the drawing for a FREE YETI Hopper 40 Soft Side Cooler!* (A $399.99 Value!) We'll give them a free Network Assessment, valued at $497!

Just email their contact information to: Josh.Wilmoth@CTTSonline.com

*Send Josh your referrals by March 31st at 8:30AM, we're drawing a winner later that morning!

## The "Not Me!" Problem... And Why This Is Almost Guaranteed TO Happen To You

Security this, password that – now they want a password with 14 characters with two symbols? And I have to change it every three months? As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code – you get the idea.

But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

## 7 Things Mentally Strong Leaders Never Do

Leaders need to stay mentally sharp to effectively lead their teams. Here are seven things that truly strong leaders never, ever do.

1. They don't mask their insecurities, but instead maintain their humility and acknowledge their mistakes and weaknesses.

2. They don't go overboard with their emotions. Instead of suppressing their feelings, real leaders stay aware of how their emotions influence their behavior.

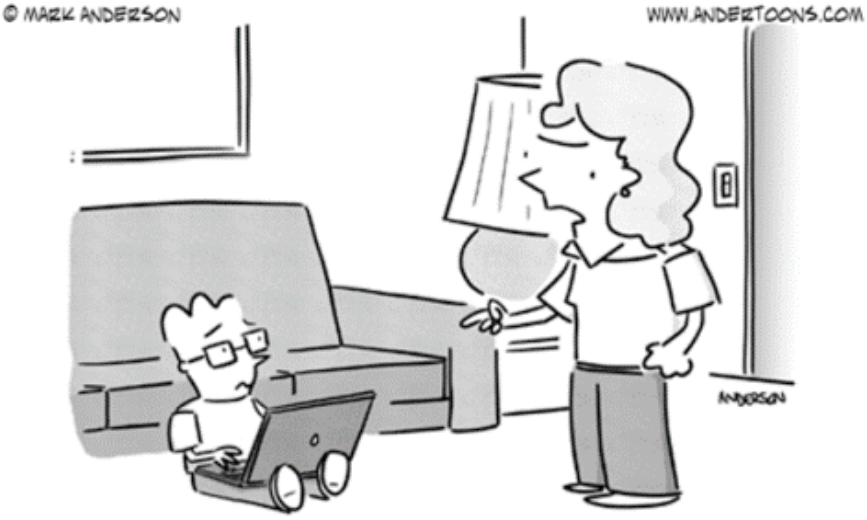
3. They accept criticism with open arms. Instead of protecting a fragile ego, mentally strong leaders take unfavorable feedback and use it to improve their processes.

4. They take responsibility for their actions. When a good CEO messes up, they apologize with sincerity and accept the consequences of their behavior.

5. They don't mistake kindness for weakness. Offering extended bereavement leave isn't letting your employees take advantage of you – it's a common courtesy.

6. They don't confuse confidence with arrogance. Though they're sure of themselves, a good leader recognizes the necessity and competence of their team. They don't put themselves over others.

7. They don't fear other people's success. When someone else is doing great things, they know that it doesn't diminish their own accomplishments.
*Inc.com 12/12/2017*




"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back

## Follow us on Social Media!

- Twitter: bit.ly/CTTS-Twitter
- Facebook: bit.ly/CTTS-Facebook
- Instagram: bit.ly/CTTS-Instagram
- LinkedIn: bit.ly/CTTS-LinkedIn
- YouTube: bit.ly/CTTS-YouTube