The Computer Center
1 Parker Pl Suite 655
Janesville, WI 53545

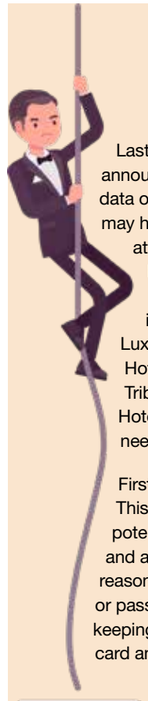
## Inside This Issue

3 Ways Your Employees Will Invite Hackers Into Your Network | 1

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now | 2

What is SEO? | 3

# 4 Steps To Protect Your Business After The Marriott Data Breach



Last November, Marriott announced some bad news: the data of up to 500 million customers may have been compromised in an attack. If you travel regularly for business and are a customer of the Marriott chain – including Westin, Sheraton, the Luxury Collection, Four Points, W Hotels, St. Regis, Aloft, Element, Tribute Portfolio and Design Hotels – there are some things you need to do.

First, change your passcodes. This should include your potentially compromised account and any accounts that, for some reason, still use the same login or passcode in 2019. Then, start keeping a close eye on your credit card and bank accounts. You may even want to consider freezing your credit. Finally, be very careful about opening e-mails. Cybercriminals love piggybacking on actual customer contacts from big corporations to send out phishing e-mails.

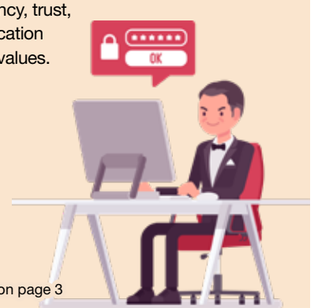
*SmallBusinessTrends.com, 12/13/2018*

### 3 WAYS TO TURN YOUR CULTURE INTO A COMPETITIVE ADVANTAGE

It's easy to focus on metrics like profit and market share when you're working to succeed. But when you fixate on these numbers instead of the people in your organization, folks start to feel like nothing more than cogs in the machine.

According to a recent study by FTSE Russell, all the companies that have received the prestigious "FORTUNE 100 Best Companies to Work For" have a single thing in common: keeping employee experience at the top of their list of priorities. These companies have stock market returns up to triple than the market average and lower turnover rates than their competitors.

But what does turning your organization into one where "employees come first" actually look like? The first step in this massive undertaking is to pick a "champion" who understands the goals of the project and the value of their team. Then, they can begin to assess where the problems are in areas like your mission, transparency, trust, communication and core values.




Continued on page 3



608-755-1524 www.computer-center.com

# THE TECH CHRONICLE

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

## *Powerful*
### By Patty McCord


As the chief force behind the unique, high-performing culture at Netflix, Patty McCord knows a thing or two about building the best teams in business. And in her book *Powerful: Building A Culture Of Freedom And Responsibility*, she lays out how to motivate the people in your organization.

According to McCord, the incentive doesn't come as a result of hollow promises and perks, but rather from challenging work and personal accountability. Instead of wasting your time and resources conducting annual performance reviews, she outlines how you can get everyone working toward the same massive, moon-shot goal. That way, everyone feels empowered, excited and ready to do something great – together.

## March 2019

This monthly publication provided courtesy of *James Pearson,* President of *The Computer Center.*

**Our greatest weakness lies in giving up. The most certain way to succeed is always to try just one more time.**
**~ Thomas A. Edison**



# 3 Ways Your Employees Will Invite Hackers Into Your Network

### ... And What You Must Do To Prevent It TODAY

No matter how professional they are, members of your team – yourself included – are going to make mistakes. It's true of every organization on earth. They'll spill scalding coffee into the company copier. They'll work overtime until the office is empty, then head home without thinking to arm the security system. They'll neglect key accounts, muck up workflows and waste hours developing convoluted solutions to simple problems. And, worst of all, they may unknowingly bumble into the cyber-attack that forces your business to go belly-up for good.

In the majority of cases, that will be by design. There's a saying in the cyber security industry, coined by renowned cryptographer Bruce Schneier: "Only amateurs attack machines; professionals target people." When it comes to repeating the same process safely and autonomously, machines are less fallible than the average person sitting at a desk. Savvy hackers looking to boost funds from unsuspecting small businesses know this. So instead of developing a complex program that dances around the security measures baked into sophisticated modern technology, they target the hapless folks on the other side of the screen.

The strategy works disturbingly well. According to IBM's 2018 X-Force Threat Intelligence Index, more than two-thirds of company records compromised in 2017 were due to what they

Continued on page 2

... continued from cover

call “inadvertent insiders” – employees who left the front door wide-open for the bad guys without even realizing it. Negligence, lack of awareness and sheer bad luck put the best-laid plans to shame on both sides.

But how does it happen? There are three primary causes of employee-related breaches, each of them contributing to a sizable portion of hacks across the country.

### 1. SOCIAL ENGINEERING

Phishing remains one of the most prominent strategies deployed by hackers to lift data from small and midsize businesses. The majority of these attacks stem from an employee clicking on a suspicious link that is embedded in a dubious or absolutely convincing e-mail. To lure your team into the trap, cybercriminals often use data gathered from cursory investigations of your organization from the Internet or social media. Maybe they pose as a security expert contracting with your company or a member of a customer support team behind one of your employees’ personal devices. Whatever mask they wear, it doesn’t take much to convince an uninformed individual to click on anything at all, resulting in a high success rate for phishing attacks.

> **“Negligence, lack of awareness and sheer bad luck put the best-laid plans to shame on both sides.”**

### 2. CIRCUMVENTED OR INCORRECTLY IMPLEMENTED SECURITY MEASURES

Even if you do everything you can to protect your business from digital attack, your team may just dodge those measures anyway. According to a report by cyber security firm Dtex Systems, around 95% of companies have employees who will attempt to override previously implemented security processes. And that’s if the security measures are configured, patched and installed properly in the first place. The IBM X-Force report lists “misconfigured cloud servers and networked backup incidents” among the chief concerns of last year.

### 3. INSIDERS WITH MALICIOUS INTENT

Hell hath no fury like an employee scorned. A strikingly large number of breaches come not from error at all, but from insidious tactics by disgruntled employees or undercover criminals looking to make a quick buck. It’s not quite a “you can’t trust anyone” scenario, but there are definitely folks out there who would sell your business right out from under your nose.

With each of these in mind, it’s vital that you incorporate extensive employee training and vetting protocols to maximize their cyber security know-how. In addition, you need to implement safe practices that reduce the room for human error, alert employees when something is amiss and protect them from the worst.

We can help. It’s difficult to overhaul your cyber security, especially on the people side, without a round-the-clock team dedicated to pinpointing the weaknesses in your organization and working to patch them up. In 2019, human error is poised to take an even more central role on the stage of digital crime. Don’t leave it up to chance. Partner with an organization that has extensive expertise in training employees on security basics and bolstering your defenses, and head into Q2 knowing your most precious assets aren’t up to the whims of an unlucky employee.

## 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 eye-opener 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. www.computer-center.com/cyberaudit/

**To get started and claim your free assessment now, call our office at 608-755-1524.**

## Cartoon Of The Month






... continued from page 4

Soon they’ll enlist the team on the project, creating regular rituals that reinforce your budding company culture. After a firm, long-term commitment to a new culture, you’ll find your company, and the people who drive it, to be healthier than ever. *Inc.com, 12/2/2018*

### SCANNING DOCUMENTS HAS NEVER BEEN EASIER — HERE’S HOW

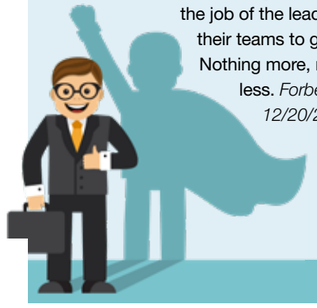
Apple’s iOS 11 app is full of exciting new tricks, but the most useful one is a little buried and definitely a lot less glamorous than most: the document scanner inside the Notes app. You no longer need to use a third-party app to upload your documents; you can do it inside Apple’s excellent internal solution.

Just open up Notes, hit the “+” symbol above the keyboard, and tap “Scan Document.” Then all you need to do is select your settings, point it at whatever document you’re trying to digitize and it’ll do the rest. It’ll optimize the picture as a scan and make the document as readable as possible. *TheVerge.com, 8/26/2018*

## The ‘Heroic’ Boss Is Obsolete

We’ve all been fed the line about the heroic boss: the Silicon Valley visionary who predicts and creates the world of tomorrow on the fly. But paradoxically, we’re also told that these geniuses are essential for the company’s daily operations.

Today’s leaders need to think differently than idols like Steve Jobs or Elon Musk. Instead of “saving the day,” the measure of a great leader should be one thing: can your team do the job autonomously? Creating great teams can make or break an organization, and it’s the job of the leaders to spur their teams to greatness. Nothing more, nothing less. *Forbes.com, 12/20/2018*



# What is SEO?


"SEO" is a term that gets tossed around like a hot potato, yet it's widely misunderstood. Unfortunately, if you don't know how it works, you can't effectively use it for your benefit. Here's a brief overview of what SEO is and why it's all the buzz in the marketing world these days.

**What Does "SEO" Mean?**

SEO stands for Search Engine Optimization and is an effective way to bring quality traffic to your website. It's the practice of using techniques like keyword optimization, social metrics and link-building to give your website better visibility in search engine results. Think of it as the digital world's new version of the Yellow Pages. If you want people to be able to find your business in the Yellow Pages, you must do the work up-front to make sure your business is listed there. The same is true for online search results. Your web page won't automatically show up within the first few pages of search results unless you work hard to get it there.

**SEO Tools**

There are a variety of tools that can help you with your SEO campaign. The goal of these tools is to help your webpage rank within the first few pages of search engine results when customers type in relevant search queries. A few of the more popular SEO tool options include:

- **Keyword Optimization:** Also known as keyword research, keyword optimization is the act of using strategic keywords to drive quality traffic to your website from search engines. It's important to only use keywords that actually relate to your products and/or services and are not misleading in any way. Keyword optimization can be used on your web page, in social media posts, and in other types of content (blog posts, press releases, etc.).
- **Links:** Every good SEO campaign should use internal and external links to guide traffic to the intended website. Keep in mind that the quality of the links must be good or your page will not rank well and could even be flagged by search engines.
- **Social Media Metrics:** When you create quality links and they're shared frequently on Twitter, Facebook, Google, etc., your content will rank higher in search results than content that isn't shared or tweeted by others.

A well-crafted SEO campaign should use a combination of these tools to ensure the highest possible ranking and visibility. Utilizing Search Engine Optimization takes effort, but it doesn't require you to pay for advertisements. Since you don't have to pay for the traffic you guide to your website through SEO, it's referred to as "organic traffic".

Contact us with any questions you have or to clam your free 30-minute consultation at:
**https://getdigitallyfit.com/contact-us**

*Janis Henslee is an Entrepreneur & CEO with an MBA in Internet Marketing. She has 20+ years' success in Marketing & Sales and 7+ of Digital Marketing Consulting. She has helped hundreds of businesspeople successfully market their business online with Branding, Graphic Design, Website Design, SEO and Social Media. Janis helps Business Owners and Marketing Coordinators develop a comprehensive strategy using the internet to grow their business and build their brand. Contact her at j.henslee@getdigitallyfit.com or 608-999-1474. Check out her website at getdigitallyfit.com and book a free 30-minute consultation.*