ALL THINGS TECH Brought to you by SYSCON

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

What's New

We have two new infrastructure projects slated for September. The first one, scheduled for September 2nd, is our fiber line upgrade which will give us even more bandwidth! The second is an internal switch that needs to be replaced. The whole team is working together to minimize work interruptions. We're sending details to our primary contact person at each client.

We are now running S100C in the Azure cloud! After months of planning, it's finally here. Our day-to-day accounting entries are all happening in our new Azure environment. Watch for updates and stay tuned.

Be careful out there, and be kind! - *Catherine Wendt*

September 2020

This monthly publication provided courtesy of Catherine Wendt, President of Syscon Inc.

We love this stuff! We are committed to helping businesses use technology to run their organization successfully and profitably.

Why Your Business Is The PERFECT Target For Hackers...

And What You Need To Do NOW To Protect Yourself

Everybody gets hacked, but not everything makes the evening news. We hear about big companies like Target, Home Depot, Capital One, and Facebook getting hacked. What we rarely hear about are the little guys – the small businesses that make up 99.7% of employers in the United States, according to the Small Business Administration. It's these guys who are the biggest targets of cybercriminals.

Basically, if you run a business, that business is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after everybody. In 2018, a cyber security survey by the Ponemon Institute found that 67% of small and midsize businesses in the U.S. and U.K. were hit by a cyber-attack.

For the cybercriminal, casting a wide net makes the most sense because it gets results. It puts them in a position where they are able to extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity, and reputation of others.

Why do cybercriminals love to target small businesses? There are a handful of reasons why small businesses make sense to attack.

1. Small Businesses Are The Most Vulnerable. Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyberthreats, or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cyber security can take a back seat to other things, like marketing or customer support. This also means they might not be investing in good network

Continued pg.2

(continued from page 1)

security or any IT security at all. It's just not top-of-mind or they may feel that because it's never happened to them, it never will (which is a dangerous way of thinking).

2. Small Businesses Don't Take IT Security Seriously. Coming off that last point, it's true that many businesses don't properly secure their network because they feel that they *aren't* vulnerable. They have the mindset of "It hasn't happened to me, so it won't." Along those same lines, they might not even take password security seriously. According to research conducted by Trace Security, upward of 80% of ALL breaches come down to one vulnerability: weak passwords! Even in 2020, people are still using passwords like "12345" and "password" to protect sensitive data, such as banking information and customer records. Secure passwords that are changed regularly can protect your business!

3. Small Businesses Don't Have The Resources They Need. Generally speaking, medium to large companies have more resources to put into IT security. While this isn't always true (even big companies skimp on cyber security, as the headlines remind us), hackers spend less time focused on big targets because they assume it will take more of their own resources (time and effort) to get what they want (money and sensitive data). Many small businesses lack the resources like capital and personnel to put toward IT security, so hackers are more confident in attacking these businesses.

> **67% of small and medium-sized businesses in the U.S. and UK were hit by a cyber-attack."**

Just because you haven't had any major problems for years – or at all – is a bad excuse for not maintaining your computer systems. Threats are growing in number by the day. While many small businesses might think, "I don't have the time or resources for good security," that's not true! You don't need to hire IT staff to take care of your security needs. You don't need to spend an arm and a leg securing your network. IT security has come a LONG way in just the last five years alone. You can now rely on IT security firms to handle all the heavy lifting. They can monitor your network 24/7. They can provide you with IT support 24/7.

That's the great thing about technology today – while many hackers are doing everything they can to use technology against us, you can arm yourself. Start with the basics: get rid of Windows 7 machines; mandate good passwords; sign up for our Dark Web monitoring to stay on top of compromised credentials; get rid of out-of-date Server Operating Systems.

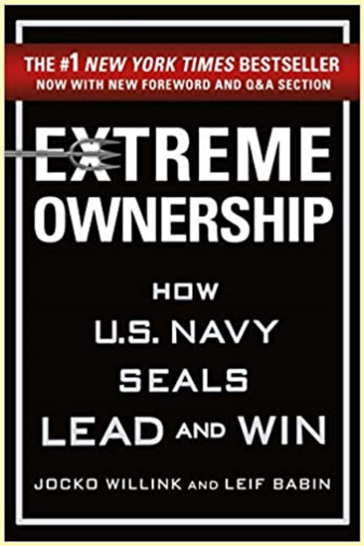
We're here to help you with all of this! Just give us a call. ☺

Cathy and Larry Sightings

It's been a month of 'togetherness.' We performed in a 'live' chamber event with some excellent musicians. This was broadcast through the Paradise Valley Chamber Facebook page (check it out!). Then, three days drove together from AZ to IL. Listened to lots of CD's and did lots of talking.

> *'Do your best, no matter how modest the task is.'*
> - Dick Capen

Extreme Ownership by Jocko Willink, Leif Babin


THE #1 NEW YORK TIMES BESTSELLER
NOW WITH NEW FOREWORD AND Q&A SECTION
EXTREME OWNERSHIP
HOW U.S. NAVY SEALS LEAD AND WIN
JOCKO WILLINK AND LEIF BABIN

In recounting their intense missions in the US effort to re-take Ar Ramadi, Iraq, these two Navy SEAL leaders weave together their intense SEAL training with the lessons that brought them success in these difficult venues. They share their experiences with their teams, leadership successes and failures, and the ownership concept.

The format keeps the book moving along. Reading the SEAL stories in difficult conditions is riveting. Added to that were the many ways the SEALs coordinated with other US agencies such as the Army, Navy, and Marines, as well as the need, and ultimate success, of incorporating Iraqi soldiers. Both authors tackle different topics, share a story from the Ramadi effort, then share the concepts as they play out in various businesses that they've worked with. They have a leadership training program that has been modified from their SEAL leadership training, specific to the business community.

Some of the chapters' topics are Extreme Ownership, No Bad Teams, Check the Ego, and various combat styles. Every team leader, junior team leader, in business or personal organizations, will benefit from this book. Go for it! - *CMW*

Shiny New Gadget Of The Month:

Weber Connect Smart Grilling Hub

Grilling can feel like guesswork. You throw the food on the grill and keep a close eye on it, hoping for the best. Say goodbye to guesswork and overcooked steaks with the Weber Connect Smart Grilling Hub.

The Weber Connect takes the thermometer and timer into the WiFi era. It monitors your food and sends updates to your smartphone. It lets you know when to flip the burgers or steaks – and then notifies you again when it's time to take them off the grill. You can even have the Weber Connect tell you when your meat of choice has reached your ideal level of doneness. It's great for those who are new to grilling or don't grill often, and it works with every grill! See more at **bit.ly/3eTL69Y**!

From the Techs

Garmin Hacked

You might be one of the millions of people who track their exercise activity through Garmin devices. So, did you notice that the free Garmin site was down for several days? Larry wanted to upload his bike rides, but the site was down—and the next day, and the next day; very unusual.

Turns out their systems were hacked and Garmin was held hostage—not just one system, a lot of their systems, including their smartwatches and aviation products. Not only were the serious exercise trackers unable to log in, but other products were impacted, including required daily uploads of data from pilots.

I'm sure there'll be more in the news in the coming weeks, but they finally reported that they paid, are you ready, a $10 million ransom to the hackers to get their data back. The rumor is that the hackers were part of the Evil Corp, a Russia-based hacker group.

Funny how many users of this 'free' software were so incensed when it wasn't available—people, it's 'free.' A bigger question should be whether the 'hack' resulted in any of their personal data being compromised. As of the most recent news reports, this has not been answered yet, only that the data was held for ransom.

So, if you have online data that's important to you, consider what you would do if the information wasn't available tomorrow. How would you know what checks you've written, or get at your contact info. You should also protect your online user accounts and change your passwords. Consider signing up for our Dark Web scanning service, and stay on top of your digital world. The Dark Web monitoring looks for any compromised passwords, personal info (answers to those security questions you fill out), anything associated with your email/domain account. It's quite sobering to see your password out there for sale!

If you have online information that is critical to you and your family—personal bank information, insurance, utilities—make sure you have a Plan B in case something happens. If tomorrow this information was no longer available, how would you get this critical information? - *CMW*

Office Upgrades—The Clock Is Ticking

We recently shared a Microsoft update that Office 2010 is end-of-life in October. That means no more patches, making this old version of Office a security risk.

Well, it's also been announced that Office 2013 will not work with Microsoft 365 as of October, either.

Bottom Line: Upgrade your Office! This might be a good time to consider moving to the monthly subscription model rather than purchasing the Office software upgrade. In fact, it's getting harder and harder to purchase Office; Microsoft really wants you to move to the 365 platform.

Great news—we've made this switch at Syscon and can tell you about your options. If you're using Teams, paying for Drop Box, and have older versions of Office, there are some really nice options available to you. Give us a call and we'll walk through them with you and see what's best. - *CMW*

Construction Corner

CFMA Issues their Recommendations Regarding PPP Entries

Lots of buzz about the PPP Loan funds. Here are some things we've seen, so get with your CPA and ***ask questions***.

CFMA—the Construction Financial Managers Association—confirms that the PPP Funds are a loan and should be treated as such.

- These should be booked on the balance sheet as a liability (a loan).
- Accrue interest at the government-specific rate.
- Even if you think some or all of the funds will be forgiven, until they are legally released, or the loan is repaid, it should be reflected as a loan on your books.

Disclaimer: We are sharing our findings with you. Our goal is to keep you informed and help you bring good questions to your tax professional. Since all of this is new to everyone, and there are regular changes coming from the government, we encourage you to research all information you find, and all answers you receive, weighing them carefully before making a decision.

Recently a CPA asked for an entry to book the portion of a PPP fund as Other Income. Based on everything known at this time, the amount he asked to have booked should meet the forgiveness guidelines. His reasoning was that the expenses under the PPP Funds will not be deductible, although he says he thinks this will change. This seems risky to us:

- It's unclear how the 'forgiven' funds will be presented on the financials and we haven't seen a final word yet.
- There are tax implications if forgiven funds are booked as Other Income.
- One source suggested treating the forgiven funds as a Gain/Loss entry. Again, there are tax implications if this is the case.
- Perhaps the forgiven funds will be posted to the Owners' Equity Section of the balance sheet. This leads to a question on how this would play out on a tax return, at a minimum.
- The payroll expenses to perform the job-specific work are absolutely part of getting the work done, without which, there would be no income, nothing to bill. So we do not think any entries should be made to reduce payroll expenses. The work performed results in the end product which is billed, so the billing and expense should remain as-is.

One final thought that you can bring to your tax professional. If you are asked to reduce expenses, do NOT reduce job-specific expenses. This will create havoc with your Gross Profit info, Cost to Complete reporting, and Over/Under WIP reports. If you have to make an entry to reduce expenses, which we are NOT recommending, use a contra account rather than posting against any specific job. This will isolate the dollar amount and keep your job-related numbers intact. More to come, I'm sure!!! - *CMW*

Who Wants To Win a $25 Amazon Gift Card?

This month's trivia question:

Who designed the first small computer for home use?

a) John Blankenbaker b) Steve Wozniak c) Chuck Peddle d) Steve Leininger

To enter: Go to www.Syscon-inc.com/Trivia and type in your answer. All correct answers will be put into a fishbowl and we'll randomly draw the winner. The Winner will be contacted shortly after the deadline and will be announced in next month's newsletter.
Deadline: September 21, 2020

Congratulations to last month's Trivia Contest winner, Carolyn Brister with **Momentum Mechanical** in Fort Worth, TX! Carolyn's name was drawn from the fishbowl for last month's correctly answered question:

Computer viruses are identified using patterns called what?
b) Virus Definitions
Visit www.syscon-inc.com/Trivia for contest rules.

Generating Passwords (Fun!)

Dave shared a fun website—DinoPass.com. It's an awesome password generator, targeted for kids, that generates random complex passwords anyone can use. It's fun and creative!

FIT

FIELD INTEGRATED TIME SYSTEM

Learn to Love Your Mondays

Are you the most expensive **babysitter** you know? We have the solution; we can show you how to get your time back!

Join us Friday, **September 25th at 11:30am Central Time!** Register at www.syscon-inc.com/events.