ALL THINGS TECH

Brought to you by ⬤SYSCON

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

What's New

The Syscon team met in August for our annual State of the Company event. The department presentations were fun and informative, and the food was excellent. Thanks to all!

We have a new security offering that monitors compromised user names and passwords associated with a company's domain name. The initial testing has been amazing! Please watch for more details. You will be stunned!

We have a new staff member we can't wait for you to meet. Misty Palek is a seasoned Sage 100 Contractor support person, with great energy; Welcome!

- Catherine Wendt

September 2017

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

We love this stuff!
Our passion is helping businesses use technology to run their organization successfully and profitably.

Data Encryption:
A Lesson From The Recent Past

In today' s world of rampant cybercrime, every savvy business owner knows the necessity of locking down their data. However, we find that the cyber security technologies used by the vast majority of businesses are woefully out of date. Sure, your current solution may have worked great, but digital threats to the safety of your company are constantly evolving. Criminals will eventually attempt to breach your data — and your barriers are not as secure as you might think.

Before World War II, the Germans developed a technology that would prove to be a key player in the conflict: its family of infamous Enigma machines. These devices, about the size of a small microwave, were composed primarily of a typewriter and a series of three or four rotors. By using a set of rules

contained in a corresponding codebook, German soldiers would use the machine to encode vital messages to be sent covertly over the airwaves. The number of potential permutations — and thus solutions — for the code was in the tens of millions. The Germans were confident that the code could never be broken and used it for a vast array of top-secret communications.

The code's impenetrability didn't last. Via photographs of stolen Enigma operating manuals, the Polish Cipher Bureau reconstructed one of the stubborn Enigma machines, internal wiring and all, enabling them to decrypt the Wehrmacht's messages from 1933 to 1938. Facing an impending German invasion, Poland decided to share these secrets with the British. But, at the outbreak of the war,

the Germans increased the security of the Enigma initiative by changing the cipher system daily. In response, a British code-breaking team, led by genius English computer scientist Alan Turing, constructed primitive computers, known as "bombes," that allowed them to decrypt the incredibly complicated ciphers faster than ever before. But it wasn't until the capture of the U-110 warship and the seizure of its Enigma machine and codebooks that the British were able to decrypt the most complicated cipher of the war, the Kriegsmarine Enigma.

The information gleaned from these decrypts are believed to have shortened the war by more than two years, saving over 14 million lives.

Just like you, the Germans believed the systems they had put in place to defend their secrets were impenetrable. And it's true: the system had few cryptographic weaknesses. However, there were flaws in German procedure, mistakes made by Enigma operators, and failures to introduce changes into the Enigma formula — along with the Allied capture of key equipment and intelligence — that ultimately allowed the Allies to crack the code once and for all.

Take this as a cautionary tale: the most advanced, complex cryptography system in the world became obsolete within 10 years. The same goes for your potentially outdated cyber security measures.

Though they may not be led by Alan Turing and his crack team, you can bet criminals are constantly chipping away at the defenses of even the most powerful firewalls. The arms race between cyber security companies and cybercriminals rages on behind the scenes, and you can bet that they've already cracked your business's "Enigma." Just look at the massive European cyber attack this past June, which infected computers from over 27 companies across the continent, including those of the largest oil company in Russia, with ransomware. The unimaginable cost of that attack is something you certainly don't want your business to shoulder.

As technology evolves, so does crime. New threats arise each and every day. While solutions are available (and needed), they are notably absent in older software developed at a time before these constantly morphing attacks even existed.

Once the enemy has found a way to pick your lock, you need a new lock. Luckily, you have your trusty IT provider, constantly on the lookout for cutting-edge solutions that protect our clients from even the nastiest malware.

Cathy and Larry Sightings

Catherine was invited to contribute an article to a special Cyber Security issue of the Business Ledger newspaper which ran August 21st.

Larry enjoyed some time with Paul Webber from Family Policy Alliance (formerly Citizen Link), a fellow Arizona resident.

'The road to success is always under construction.'

- Unknown

The Coaching Habit: Say Less, Ask More & Change the Way You Lead Forever

This book by Michael Bungay Stanier talks about a coaching style versus a management style as we engage with our staff, and when the coaching style is appropriate and actually beneficial. As with anything of value, it takes time and thought, but the results may be worth the effort.

He starts with 7 Essential Questions, then discusses 5 Essentials to build a new habit of using those 7 Questions in your daily interactions with staff. I'm sure you wouldn't be surprised to hear that when you try something new, you'll get resistance, no matter how good it is. Consistent use is the key.

Recommended: This book is definitely worth your time—*CMW*

The Coaching Habit Say Less, Ask More & Change the Way You Lead Forever
Michael Bungay Stanier
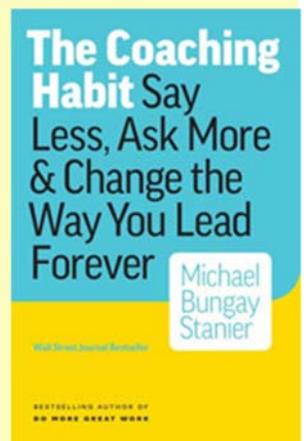
Shiny New Gadget Of The Month:

Building A

The cutting-edge U by Moen Smart Shower is looking to revolutionize your shower experience. With digital valves and a corresponding controller, the U by Moen can make any shower a lot smarter.

After users install the digital valves and controller — a task that takes a few tools and a little bit of handiwork — the U by Moen allows them to sync their showers with their smartphone. The system then makes it easy to customize the showering experience, choosing the perfect temperature and saving preferences for future use. Start the shower remotely, and it will let you know when it's ready, automatically shutting off until you step in.

Available for showers with either two or four outlets, the U by Moen is the perfect addition for those looking to digitize every aspect of their home.

News From Our Techs

Secret Chips In Cell Phone Spare Parts

There's a growing trend—small cell phone repair shops are springing up all over. They usually provide repairs for cracked screens and other fixes, often at a lower cost and with a quicker turn-around than the manufacturers.

Some unsavory characters have invaded this market. Some replacement parts have been compromised with secret hardware. The devices are hijacked, logging keyboard input and patterns, installing malicious apps, taking pictures and emailing them to the attacker.

Turns out the malicious replacement parts are not very expensive and can be mass-produced. They're hard to identify as compromised, so the local repair person may not even know that the parts have been tampered with. According to an online article by Dan Goodin, ARS Technica, BIZ & IT, this is referred to as a 'chip-in-the-middle' attack.

There are more and more people using phone apps for home security, garage door access, monitoring home cameras, and many other conveniences. If that describes how you use your phone, you might consider forking out the extra money and having repairs done by the manufacturer; not necessarily a guarantee, but the odds are better.

Bank Websites, Trusteer Software, and the Truth About AV

When I log on to our bank's website, or we're troubleshooting with you, we often see the invitation to install the Trusteer software. The bank log on screens strongly encourage you to install it. So what do the Techs have to say about it?

Don't Install It! This program uses quite a bit of computer resources while it's scanning which slows down your computer. If you have an anti-virus solution installed on your computer (and you should already have this), the Trusteer software creates conflicts since it's a type of anti-virus product. They fight each other for computer resources, for one thing. The Trusteer software also interferes with our anti-virus solution and even blocks our anti-virus updates!

Banks push this solution because, in their experience, many people do not have anti-virus software installed, or it is woefully out of date. They want to protect their sites and their users' credentials, an admirable goal.

Bottom line? Do <u>not</u> install this on your business computers that already have anti-virus, and especially if you are on one of our Private Cloud solutions. Still not sure? Give us a call and we can take a look.
- *CMW*

Construction Corner

Emailing out of Sage 100 Contractor

This was a tough one! We had a client that was having difficulty emailing ACH payments and Work Orders out of the software. Their IT group had tried several things and they just couldn't figure out the answer.

Our Tech (Scott) remembered that over the years, we've seen odd problems and errors with special characters in the Note Pad and the Description fields. This specific client had been on the software for many years, so some of these characters used to be allowed (there are pop-up warnings now). He got the idea to check the Equipment descriptions for any special characters and sure enough, after the changes, the email went through!

We've also run into this with Vendor Names, Vendor Short Name fields, and copy-paste from email or Word documents straight to a field or Note Pad. We've worked with this software for over 20 years, so we have LOTS of history and experience. - CMW

Version 20—Are You Hoping It Will Go Away?

We've heard that some of you are not reading the articles or listening to the videos because you just don't want to deal with this upgrade; we feel your pain and understand, BUT, it's time to bite the bullet and dig in.

Sage has been clear that none of the reports we need in January to wrap up 2017 will be available. Lately, their support desk will not assist with any v19 issues; move to v20 and they'll help if the problem persists, they say. We really can't blame them for wanting everyone to move to v20, but if you have custom programs or reports, you need to engage right away, since everyone's in the same boat and some of these changes take time.

If you haven't had your half hour planning call with us, now's the time. At least go listen to the videos and read the articles. Everything's available on our website.

Other Stuff

Your Copier Is Spying On You

It may sound paranoid, but it's true: the machines you use every day around the office could be spying on your data. Copiers and multifunction printers, particularly, are some of the leading causes of business data breaches. When you consider it, it makes sense. They're among the only devices on the network that rarely have their default password changed. But these advanced copiers and printers often house images of all the pages they've ever scanned on an internal hard drive, making them the perfect target for thieves. Make sure to change the password from the default on every network-connected device in your office. This one simple step can save you a costly headache down the road. *intellisystems.com 01/31/2017*

sysconfidence✓

Every business needs it; do you have it?