

ALL THINGS TECH

Brought to you by  **SYSCON**

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

What's New

The holidays are behind us. Many of us are compiling information for our Accountants as we look ahead for tax filing. The stores are filled with candy heart boxes and roses!

Back at the office, we've just installed additional data storage for our clients, and replaced ours, as well. Next up is an upgrade of our Firewall in anticipation of enhanced security changes.

Our offer to scan your domain name for compromised user names and passwords has caused a few people's hearts to skip a beat when we showed them their password, out there for sale. Haven't checked it out yet? Just give us a call!

- Catherine Wendt

February 2018



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.



Cybercrime: Size Does NOT Matter

Though we're in the midst of an unprecedented rise in high-profile cybercrime incidents, it's easy to assume that our own much smaller businesses are safe. Sure, we think, hacking into the data stores of J.P. Morgan, the U.S. Government, or Virgin America can net hackers millions and millions of dollars. Why would they bother with a small business?

But unfortunately for all of us, hackers actually *do* bother with small businesses across the country – these attacks just don't make the news. By some estimates, including one reported in Media Planet, more than half of small businesses have had their data compromised. According to StaySafeOnline.org, these attacks, targeting small to midsize companies, now comprise over 70% of all data breaches.

What's worse, this digital onslaught shows no sign of slowing. In fact, ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime.

Once you see these numbers, it's easy to understand why hackers seek the little guy. These days, massive corporations like Google or Citigroup employ incredibly sophisticated digital measures. Their digital vaults, though containing ludicrously attractive sums of potential money to grab, are located at the end of a virtual labyrinth covered in traps, with a final, inches-thick steel door protecting their assets for good measure. In contrast, the digital assets of small businesses are often hidden behind nothing more than a single, often weak, password. With thousands of

Continued pg.2

(continued from page 1)

business owners going about their day-to-day, utterly oblivious to their paper-thin security, the question turns from “Why would hackers bother with my small business?” to “Why *wouldn't* they?”

Though cybercriminals may come away with less than they might have had they targeted a Fortune 500 company, it certainly isn't going to seem cheap to you. According to one TechRepublic analysis, an average cyber-attack on a small business can cost as much as \$256,000. Is that a sudden cost your company can weather?

Luckily, there is hope. Though small business owners often assume that effective cyber security solutions lie far outside their budget range, robust digital secu-

urity is now more affordable than ever. By investing in comprehensive protection, small businesses can deflect even the most persistent hackers.

Today, a cyber-attack on your business is almost statistically inevitable. And when that attack comes, you'll definitely want to be prepared.

If you haven't needed a doctor for the past two years, does that mean you're going to abandon your health insurance coverage? Of course not. What about car insurance? Does it become unnecessary in the absence of a crash? No, because even if you're the best driver in the world, sometimes a collision is out of your control.

What's more, both your body and your car require regular upkeep and maintenance to remain in

peak condition. It's no different with your network security. As technology advances forward at an

ever-increasing speed, the ways that hackers can infiltrate your network continue to multiply. The best digital security platforms constantly update, enabling them to anticipate these shifts and prevent them from becoming liabilities. This way, you can be proactive prior to a digital crisis, ensuring that no matter what comes, your network is protected.

Invest in regularly maintained, powerful cyber security, and ensure the future of your company. Let's look at end-of-life equipment, automated patches, and other tools to keep you safe!

Cathy and Larry Sightings

Catherine attended an industry conference in Phoenix, AZ.

Larry beat last year's individual and team time trials with the Strada Bike Club.

'If you need me to motivate you, I probably don't want to hire you.'

- Daniel Pink

“What's worse, this digital onslaught shows no sign of slowing. In fact, ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime.”

Have You Ever Read The Whole Bible?

In High School, I helped teach CCD on Saturday mornings and went to class myself, but hadn't read any book of the Bible until I was in my early twenties. Now as I read modern literature, fiction, magazine articles, and listen to the news, I'm reminded just how much those Proverbs, Parables, and Stories show up as references – and these go right over the heads of our kids and employees!

These books are filled with wisdom; how to handle confrontations; how to be a great spouse, parent, and child; words of wisdom in Proverbs; wonderful poetry in the Psalms. Did you know that if you read three (3) chapters a day, you could make it through the entire Bible in about one year? How about one of the free App's? Are you willing? – CMW



Shiny New Gadget Of The Month:



August Doorbell

It's 3 a.m. You and your family are all tucked away in your beds, snoozing away. Suddenly, the doorbell rings, and everyone is shocked awake. Who is that? What do they want? And, most importantly, what should you do?

It's a dicey situation, but luckily, modern technology has an answer — the August Doorbell Cam Pro. Another addition to the endless list of "smart home" offerings, the device is a small, unassuming square doorbell.

At any time — say, when a dark figure is looming on your porch in the middle of the night — you can open up your phone and take a look through the August Doorbell's camera. After that, if you feel like a conversation is in order, you can talk through the device's built-in microphone and speakers. With the ability to sync up to August's smart locks and Amazon's Alexa, the August Doorbell Cam Pro is a vital and convenient security addition to any smart home. (cnbc.com)

New Security Measures for Our Hosted Clients

It seems some people with good computer skills have entirely too much time on their hands. We regularly see attempts to hack into our servers, our client servers, and our hosting environment. An example: a hacker bombards a server with automated log on attempts using guessed passwords, sometimes referred to as a dictionary attack, or a brute force attack.

You might think these attacks are all from overseas. Some of these intrusion attempts come from overseas, and we can use country-blocking to address some of them, but that's not the whole story.

There was a rather annoying hacker right here in the good ol' USA that had some 'favorite' servers to target, servers under our care. We had gotten pretty tired of this, so we added a few tools; this really ticked him off. The hacker greatly expanded the number of servers to attack and the frequency!

Why are we sharing this with you? For this hacker, it was a game, then a matter of pride. For others, it's all business; they want to encrypt the data, make the ransom request, get paid, and move on to the next one; nothing personal, just business.

Well, we're in the business of **protecting** our clients' servers and data. We have no intention of just

watching this go on.

In the coming months, we have a few tools we will layer on to our security protocols in the hosting environment.

Like an intricate clock or a great piece of machinery (I love cars), having the right components can make things just 'hum.' We know that refining access to servers, fine-tuning the firewall settings, and increasing user authentication will further limit the number of attacks, as well as the risk of a breach.

So in the coming months, if you use any of our hosting solutions—Private Server hosting, Multi-Tenant hosting—we will roll out these added features. This will include changes to the public access of the server you log into; creating a direct VPN 'tunnel' to our hosted environment; arranging additional authentication for remote users and those with laptops on the road. We'll limit the number of log on attempts, after which the user (or hacker) will be locked out for a period of time.

This is in direct response to the onslaught of attacks we're seeing, and it's where the industry is going as we all look for ways to step up security and protect our clients. We'll reach out to you with more details in the coming months! - CMW



Construction Corner



Join us Thursday **February 8th at 11:30am Central time** for our **Webinar** on migrating the prior year archives to version 20 – all of them!

What's New in Sage 100 Contractor version 20?

The **latest tax update** is here! Version 20.7.28 has the new Federal Tax Tables and is ready to install. Don't forget the new feature that pushes the update to the workstations from the Database Administrator Tool; what a time-saver!

Ever posted a Payroll Record to the wrong posting period? You can now change the posting period for a group of records!

Now you can 'hide' Inactive Employees, Clients, Jobs, even

Parts from the look up screens without having to delete anything (you should never delete employees). Pull up the list, choose Options, and walk through a few steps to check mark the Inactive items; you'll love this one.

A little irritated that any cash account entry in 1-3 comes in under adjustments? Now when you make that entry, you can choose whether it's a Deposit, Check, or an Adjustment.

All Archiving features, both Fiscal and Payroll, are handled through the new Database Administrator tool, not the 1-6 or 5-3-7 screens, respectively. The good news here is that if anyone is logged on and you need Exclusive Access, you can see who, they get a warning and a 60-second count down to wrap up and get off!

There's a new 'Refresh' button when previewing a report. If you

drill down and make a change, then choose Options, Refresh, the report will reflect the change, rather than backing out and regenerating the whole report.

I think this one is a two-edge sword – you can View the history of changes in a record. Who made the change, when, what was changed. SQL logs the changes as they're made.

The 'new' feature that won't allow a Final Compute if the employee has negative vacation hours is gone! Sage heard you and removed this new 'feature.'

For those who use Unitary Billing, the Invoice number issue is now resolved.



Collecting Time From the Field Just Got Exciting!

We're helping our clients collect field time from mobile devices, and we're fully integrated (really!) with Sage 100 Contractor version 20.

We can collect cost code information, work order numbers, phases, client signatures, and a whole lot more. Interested?

Who Wants To Win a \$25 Amazon Gift Card?

This month's trivia question: **In what year did the Wright Brothers successfully design and fly a motorized aircraft?**

a) 1900 b) 1896 c) 1910 d) 1903

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: February 19, 2018

Congratulations to last month's Trivia Contest winner, **Dennis Oster**, with **Hovlands, WI!** Dennis's name was drawn from the fishbowl for last month's correctly answered Question:

Phone phreaking was a popular hacker pastime in the 1980's. What did phone phreaking entail?

d) Hacking telephone services to make free calls