ALL THINGS TECH

Brought to you by SYSCON

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

What's New

We've been watching the leaves turn to orange, red, and brown; just beautiful! The pumpkin candy dishes are out, and we're stocked up with treats, too.

Several clients are wrapping up their construction projects which includes moving the computers and network equipment. This is a team effort all the way around; great job to all.

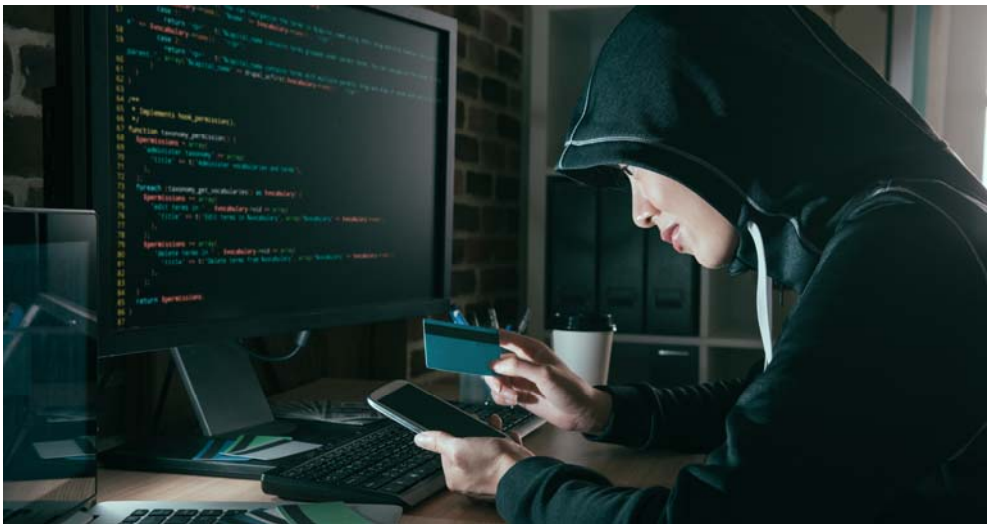
We've updated software for our CRM and VMware. After 20+ years on our TimeCard program, we just moved to our FIT System for our time collection! We're also planning ahead for the Windows 7 end-of-life (are you?).

- Catherine Wendt

October 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.



How To Make Sure You Never Fall Victim To Ransomware

Late last March, the infrastructure of Atlanta was brought to its knees. More than a third of 424 programs used nearly every day by city officials of all types, including everyone from police officers to trash collectors to water management employees, were knocked out of commission. What's worse, close to 30% of these programs were considered "mission critical," according to Atlanta's Information Management head, Daphne Rackley.

The culprit wasn't some horrific natural disaster or mechanical collapse; it was a small package of code called SAMSAM, a virus that managed to penetrate the networks of a $371 billion city economy and wreak havoc on its systems. After the malicious software wormed its way into the network, locking hundreds of city employees out of their computers, hackers demanded a $50,000 Bitcoin ransom to release their grip on the data. While officials remain quiet about the entry point of SAMSAM or their response to the ransom, within two weeks of the attack, total recovery costs already exceeded $2.6 million, and Rackley estimates they'll climb at least another $9.5 million over the coming year.

It's a disturbing cautionary tale not only for other city governments, but for organizations of all sizes with assets to protect. Atlanta wasn't the only entity to buckle under the siege of SAMSAM. According to a report from security software firm Sophos, SAMSAM has snatched almost $6 million since 2015, casting a wide net over more than 233 victims of all types. And, of course, SAMSAM is far from the only ransomware that can bring calamity to an organization.

If you're a business owner, these numbers should serve as a wake-up call. It's very simple: in 2018, lax, underfunded cyber security will not cut it. When hackers are

Continued pg.2

(continued from page 1)
ganging up on city governments like villains in an action movie, that's your cue to batten down the hatches and protect your livelihood.

The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?

1. BACK UP YOUR STUFF

If you've ever talked to anyone with even the slightest bit of IT knowledge, you've probably heard how vital it is that you regularly back up everything in your system, and it's true. If you don't have a real-time or file-sync backup strategy, one that will actually allow you to roll back everything in your network to before the infection happened, then once ransomware hits and encrypts your files, you're basically sunk. Preferably, you'll maintain several different copies of backup files in multiple locations, on different media that malware can't spread to from your primary network. Then, if it breaches your defenses, you can pinpoint the malware, delete it, then restore your network to a pre-virus state, drastically minimizing the damage and totally circumventing paying out a hefty ransom.

"The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?"

2. GET EDUCATED

We've written before that the biggest security flaw to your business isn't that free, outdated antivirus you've installed, but the naïve employees who sit down at their workstations each day. Ransomware can take on some extremely tricky forms to hoodwink its way into your network, but if your team can easily recognize social engineering strategies, shady clickbait links, and the dangers of un-vetted attachments, it will be much, much more difficult for ransomware to find a foothold. These are by far the most common ways that malware finds it way in.

3. LOCK IT DOWN

By whitelisting applications, keeping everything updated with the latest patches and restricting administrative privileges for most users, you can drastically reduce the risk and impact of ransomware. But it's difficult to do this without an entire team on the case day by day. That's where a managed services provider becomes essential, proactively managing your network to plug up any security holes long before hackers can sniff them out.

In case you think we're just 'fear mongering,' just this week I received an important notice from Bank of America regarding a deposit (I don't bank there), and from American Express about my card (I don't have one). Add in the message from a client whose personal email was just hacked, and it's a typical day.

The bad news is that ransomware is everywhere. The good news is that with a few fairly simple steps, you can secure your business against the large majority of threats.

Cathy and Larry Sightings

It was vacation time! Catherine and Larry drove from Phoenix AZ to Colorado Springs for a special event with Focus on the Family at the Broadmoor, stopping along the way in Durango, CO, and driving through the beautiful mountains. Many trees were turning colors; nights were cool, daytimes warm. Just beautiful!

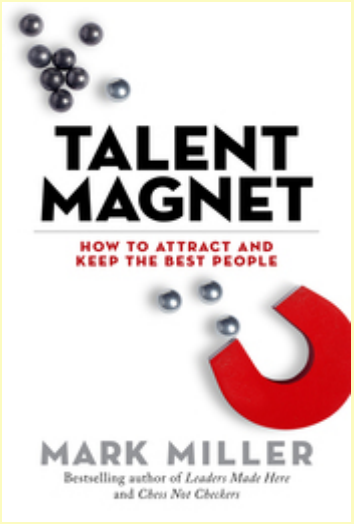
'Motivation without action leads to self-delusion.'
- Darren Hardy

Talent Magnet by Mark Miller

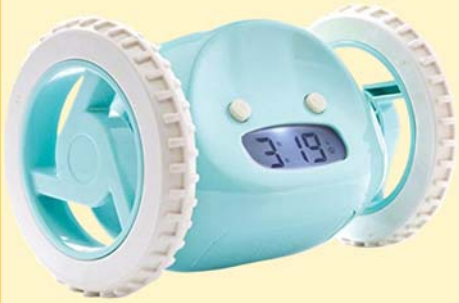
Rob from my accountability group stumbled on this book at an airport, then suggested all of us should read it; so glad he did!

The book is written in a story format. A CEO has a growing problem finding top talent, so he and his team set out to discover what attracts top talent. During this process, the CEO's son, along with some friends, are looking for summer work to raise money to help build a well in a third world country, a place they had visited. The kids set out to discover what kind of job they'd like and what kind of company they'd like to work for. Between father and son, they discover a formula—TM = B^3A; **T**alent **M**agnet equals **B**etter Boss, **B**right Future, **B**igger Vision, and **A**wareness.

The book is a little sugary, but the research and experiences are solid. The kids' experiences are great reminders, too. Recommended! - *CMW*



Shiny New Gadget Of The Month:



Clocky

The Alarm Clock On Wheels

Waking up can be difficult. Even the most driven people occasionally struggle to get out of bed in the morning, pounding the snooze button ad infinitum until we finally force ourselves upright, dazed, and groggy from interrupted sleep.

That's where Clocky, the alarm clock on wheels, comes in. Clocky is an adorable little digital timekeeper to keep by your bed; it will be your best friend until it comes time to rise in the morning. By default, it'll give you a single press of the snooze for free, but once you hit snooze for the second time, it'll speed off and start wheeling around your room, beeping and making a racket until you catch it and send it back to sleep. If you or someone you know struggles to get out of bed in the morning, Clocky will be a trusted ally in your mission to start the day.

From the Techs

Credit Card Skimmers—New Detection Tool

You've probably seen news clips talking about a compromised ATM or point-of-sale device that is being used to collect credit card or debit card credentials. These 'skimmers' capture the magnetic stripe and PIN code information.

In an ArsTechnica article by Sean Gallagher, a couple of researchers have created the 'SkimReaper' device to thwart these skimmers.

There were four types of skimmers found during the study.

- Overlays are one of the two most common. These are put on top of the ATM or PoS system and sometimes have a corresponding keypad to collect PIN info.
- Deep Inserts, another of the most common, are designed to be jammed into the card reader slots. The info is read when the card is inserted or pulled out.
- Wiretap skimmers are installed between the device and the network they're connected to, but this indicates a security problem on the network!
- Internal skimmers are more common at gas pumps. They have to be installed between the terminal and the rest of the hardware, so there's a bigger chance someone could be seen and get caught setting this up.

The NYPD and some other police agencies have signed up to use this new SkimReaper, and during initial testing, it had a 100% detection rate; pretty impressive! I still can't help but think that if all these clever crooks helped out with some of our bigger world problems, we'd all be better off!

Chrome 69 and Flash

Seems like we just got word about Chrome 68 and the 'not secure' warning for websites without SSL Certificates. Now we have news about the latest Chrome 69 release that came out September 4th.

Adobe has a Flash plugin that is used on a lot of websites. Adobe had previously announced that it is ending Flash plugin development as of January 2020, and Chrome has made changes since 2016 regarding this feature. Right now, if Flash is enabled for a site, it will continue to be so and restarts with the browser according to Peter Bright, an editor for ArsTechnica.

With the upcoming Chrome 69 release, Flash will have to be enabled for every site, every time you start the browser. The good news is that you'll absolutely know when it's running; the bad news is that you may find this added step to be annoying.

In the meantime, I logged into Chrome after a few days of vacation and once again, everything looks different, again! - *CMW*

Do you get our weekly email blasts?

These are short, **2-minute video updates** on tech-related topics. There's often a **short blog** if you want to read more on the topic. If you don't get these, **please call Jonathan** at our office and we'll make sure you're on the list. You might have to 'white list' us, and we can tell you how to do that, too!

Construction Corner

The 'Airbnb' of Heavy Equipment—There's a Missouri-based company that wants to offer heavy equipment in the same style as Airbnb. Back in 2014, some contractors got together to solve the lose-lose of either buying expensive equipment that won't be used much, or paying high rental fees. They've received some significant venture capital and they're focused! www.equipmentshare.com

Version 21.2 for Sage 100 Contractor—Earlier this year Sage released version 21.1 and we suggested you hold off on upgrading since we expected another upgrade before the yearend rolls around. Well, it's here, version 21.2. Mary sat in on the Beta features update from Sage, and here's what she learned.

Sage has added the ability to **merge two client records** together. One of the two Client records is considered the 'to' and the other is 'from.' All the details from one record are merged into the primary record, and the 'from' record is automatically marked as Inactive (fairly recent feature). The same process will work for Vendors, as well. This may come in handy.

As ACH and online payments have become a regular part of our bookkeeping lives, we often have to make 'fake' payments to clear open AP entries and update cash. Version 21.2 has added a feature to **record an external vendor payment**, indicating payment by credit card, ACH, or a manual check. We haven't seen this in action yet, but it's sounds promising.

The 3-6 Client screen has a new field, a place to **enter an email address to send statements**. When you print client statements, the ones with an email address in this field will prompt you to verify the email address, then identify which ones actually need to be printed (faxed?).

A few versions ago, Sage added the ability to create reports and report forms that are flagged as **Shared, Private, or available for a specific Company**. This has created a lot of confusion when making edits, etc. With version 21.2, the status will be part of the name of the report, so you'll know what's what!

If there's a feature you just have to have, watch for the full release in the coming weeks.

Who Wants To Win a $25 Amazon Gift Card?

This month's trivia question:

When was the first GPS satellite launched?

a) 1776 b) 1963 c) 1994 d) 1978

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: October 20, 2018

Congratulations to last month's Trivia Contest winner, **Jill Snethen**, with **Key Builders**, IL! Jill's name was drawn from the fishbowl for last month's correctly answered Question:

Which of the following websites was launched first?

d) Google

Collecting Time From the Field Just Got Exciting!

We can also collect cost code information, work order numbers, phases, client signatures, and a whole lot more. Your field can use iPhones, Androids, or Tablets. All the info is sent straight to Sage 100 Contractor, no copy-paste! What a time-saver.

Interested? Join us for a demo on **October 24th at 11:30am CT!**