Syscon U

What's New

'Tis the season of graduations! Congratulations to all, including our own Beth Kramer in achieving her MBA! Lots to celebrate.

Thank you to all of you who participated in our Net Promoter questionnaire—we hope you enjoyed the whole experience! The response rate was 43.95% (!!) and our score of 80 is 5 points higher than 3 years ago, which is about 190% higher than our industry! We have a company-wide presentation to share the findings and many kind words, then dig into the things that need attention.

Thanks to all of you who followed and encouraged the 53-day bike ride. It was so fun to have many of you tracking the journey! - *Catherine Wendt*

In this Issue

June 2021

Ransomware and Zero Trust

BIG NEWS—a ransomware attack that not only extorted $4.4 million—a ridiculous amount of money—but also resulted in a shutdown of a 5,500-mile pipeline system transporting more than 100 million gallons of gasoline, diesel, jet fuel, and heating oil per day. That's roughly 45% of the fuel consumed on the Eastern Seaboard between the Gulf Coast and the New York metro area—this got a lot of attention, for a lot of reasons!

The Colonial Pipeline is a Georgia-based company. A known hacker group targeted this company, hitting it with a ransomware attack. Basically, the hackers lock up the company's computer systems by encrypting the data. Then they demand a large sum of money, after which they 'promise' to send the code to unencrypt the data (which may or may not work, if you receive it). Ransomware attacks reportedly increased 300% in 2020 alone, in just the US—it's BIG money!

This known hacker group is a professional criminal group that has cost Western nations tens of billions of dollars in losses in the past 3 years, per a CBSnews report. They claim to be a Robin-hood-type group. They seem to think their policy to not hack hospitals, nursing homes, educational, or government targets somehow makes them altruistic—what? News alert: cutting off fuel between Texas and the North East impacts every one of these industries. Some of the news articles out there imply that the shutdown wasn't their intention, they were 'just extorting money'; as if that makes it OK or less egregious?

In the future, we'll probably get more details about *how* they were hacked. For now, news sources are saying this was related to a lack of security updates; we'll see. On May 8th, the Colonial Pipeline announced they had been

Continued pg.2

(continued from page 1)

hit with ransomware. The attack was focused on the Operations part of the business, not the fuel delivery systems, but the company shut it all down, just in case. What else could they do? They had to err on the side of caution.

A few months ago, we shared some updates from ID Agent about 3 top US breaches involving ransomware—a Minnesota healthcare system, a short line railway, and a medical lab. In these cases, they actually stole personal data, too, with the goal of selling it on the Dark Web; another lucrative business.

This kind of attack usually requires someone to have been sloppy—clicked a link that they shouldn't have; downloaded something from a website; poorly maintained equipment; weak passwords. So now there's a new concept—the idea of Zero Trust, which has been out there for a little while. We're pretty sure you're going to hear a lot more about it in the coming months. Zero Trust starts with the idea of 'never trust,' always assume a breach. If you come from a position of Zero Trust, you verify every device, application, every identity, in all cases. This is in line with the Multi-Factor Authentication (MFA) push by many businesses as they try to stay ahead of hackers and the social engineering efforts to trick people into giving up personal data or 'opening the door' in an environment. In both Zero Trust and MFA, the idea is that you have to have a second step to prove you are who you say you are.

If you Google 'Zero Trust' you'll find quite a bit of info including some Microsoft videos about the topic and how their tools are helping provide security and safety. Check out our previous articles and videos about implementing MFA, too.

So, what about your business? Could you be down for 5 days? You wouldn't know who owes you money or how much; no access to what you owe or to whom; no ability to cut checks or enter cash receipts; can't run a payroll; no access to Word docs, Excel, PDF's, drawings, pictures—all of it held for ransom. How about a $200K ransom payment? Not to mention all the IT costs to recover everything, the lost work time, and, *if* you get the data back, you have to enter 5 days' worth of data. Then, when all of this is done, you still need to make those security changes.

We have a better idea—take action now. Educate your staff on social engineering tricks, continuously; replace end-of-life equipment; replace out-of-date software; update patches and firmware on your devices; setup MFA on critical systems; be sure you have off-site backups and test that you can recover the data; get some decent passwords in place and enforce them. Need help? This is what we DO, so let's dig in! - *CMW*

Cathy & Larry Sightings

Catherine attended the C12 Currents' 21 event in Orlando; great!

Larry is getting back to 'normal life' after his cross-country bicycle trip.

"We cannot direct the wind, but we can adjust the sails."

— Dolly Parton ♬

Book Nook

Surviving the Business Storm Cycle by Dave Hopson, Ph.D.

Things get so busy you can barely keep up (dodgeball), then things slow down (baseball) and you wonder what you did wrong. There were many nice summaries of the business cycle, very clearly stated and with examples. Mr. Hopson describes this cycle as the Tornado, where you have Traction, followed by an Avalanche where things slow down and you have to clean up and you enter the Consolidation phase.

He has some very nice comparisons to the life cycle of a caterpillar, adoption of new technologies, and a few others. In each case, there's a rhythm, an expected cycle. In business, he believes it's important for a company to know what phase it is in at any point, and take action appropriate to that phase.

I really enjoyed how much time he spent talking about the opportunities built into the slower part of the cycle; the importance of bringing staff along, including training, and acknowledging the resistance to change; and finally, how technology needs to be the third part of the triangle – People, Process, and Technology.

The constant pitching of his services as an outside consultant was a little irritating. I agree that IT gets too-little attention and most companies want the 'magic bullet' and balk at investing in training, so the point is still valid. The key ideas and reminders are worth the effort; it's a fast read! - *CMW*

Cyber Insurance; Ouch!

I recently sat in on an industry-specific presentation about Cyber Insurance. We get a lot of questions about this, and the presenter was with the insurance company! Thought I'd share some info.

According to CHUB, Small Businesses under $25 million in revenue are THE target and ransomware was the top Cyber Insurance claim category in Q1 of 2020. These claims have increased 486% in the last 3 years. Insurance premium rate increases are between 20% and 50% upon renewals.

Errors & Omissions—Protects you from liabilities resulting from your mistake or failure.
First Party Cyber Coverage—covers damages due to a data breach; this can include investigative services, business interruption, and data recovery
Third-party coverage— covers damages if your customer or partners are affected by a cyber-attack on your business including legal fees, settlement costs, security failure, and media liabilities

If you want the insurance company to pay a claim, there are some new requirements in these policies: a Firewall with up-to-date firmware; End-point management (anti-virus and regular patches); backups that run without human intervention and are not connected to the network; multi-factor authentication is another we've seen.

You should be proactive with your computers and data, and continue to educate and warn your staff just to protect your business, your livelihood. Given this onslaught of hacker attempts, you should also get with your trusted insurance agent and get clarity on what policies cover which situations. Then bring the requirements to your tech group (us!) so we can talk through what you do and don't have, and if there was a claim, how we would show you were compliant.

Don't like having these additional premiums? We're with you, but you absolutely won't like paying a ransom, or losing your data if you're compromised. We have a 'fun' image on the reception-area screen when you come into our office. It's a knight in full armor and a caption about having the latest security protection software. The picture to the right shows an arrow through the small visibility slit of the helmet that says 'user clicked on link.' Get all of this in place, then be sure to keep sharing our articles, links, and warnings ! - *CMW*

Anything with a Chip, Plan on Waiting

There's a global shortage of computer chips. There are quite a few contributing factors such as supply chains; natural disasters; the pandemic (but this started before that event); changing sizes and chip standards; build time; and plain old growing demand!

Computer chips aren't just in our laptops, workstations, and servers; they're in our phones, cameras, printers, and a growing number of devices for work and fun. The manufacturing places are called 'Fabs' and have specific requirements to keep out dust, maintain temperatures, and avoid static charges. They take a LOT of money and 2 years to build. All existing Fabs are running at full capacity and can't keep up. Expect prices to increase, too.

So if you're going to need a new computer, or a car, you might find yourself on a waiting list, so plan ahead! We don't see this changing in the near future. - *CMW*

Shiny New Gadget Of The Month:

Ambient LED Outdoor Bluetooth Speaker

Summertime is upon us! That means we'll need a way to bring some tunes outside with us.

TikiTunes has a portable Bluetooth speaker that's water-resistant and dust tight. The speaker has a flame-like effect to make it look like it's lit by flames. Two speakers can by synced together. Speakers connect to any mobile device with Bluetooth. TikiTunes recommends keeping the device less than 6 feet away from the speaker (or speakers) without any objects between them for best quality. The maximum range is 30 feet.

The battery lasts up to 6 hours on one charge. The rechargeable battery comes with a micro-USB cable. It takes 2.5 hours to fully charge the speaker. Each speaker weighs 0.88 pounds and is 4" x 4" x 7."

Learn more at: https://www.thegrommet.com/products/tikitunes-ambient-led-outdoor-bluetooth-speaker

Construction Corner

Tracking Items to be Reimbursed by Others

There are a couple of scenarios where you have company or job-related expenses that need to be reimbursed by others. Happy to share a few of the most common requests we receive.

Personal Items on the Company Credit Card—So you open up the credit card statement and notice that one or more people put personal items on the company card. How are you going to track what they owe so you can be sure it's reimbursed?

In the entry screen (4-6 to enter the statement details, or 4-7-3 to enter credit card receipts), use an Asset account with subaccounts. You can use the Employee Loans account, or create one with a different name. In either case, set it up to require Subaccounts. Use the Employee's number as the subaccount number to keep things consistent.

If the employee pays you back (cash or a check), in the grid of the 1-2 Deposit screen, enter the same Asset account and employee subaccount. If you're going to take the money back as a payroll deduction, run the 2-4-51 Subsidiary ledger for the Asset account before you start payroll so you have the amount. Then on the Calculations tab of the 5-2-2 screen, use a Pay calc that is specifically setup to post to the same Asset account.

When you re-run the 2-4-51 report, you'll see all the activity and the net amount due after posting payroll.

Job-Related Permits, Bonds—In some contracts, the Owner has agreed to reimburse you for the permit or bond. You have a rough idea of the cost, but not the final number. You order what's needed and now you have to enter it and track that you're reimbursed.

> *'This helps keep the responsibility with your Project Manger, since they have access to the Job Cost reports.'*

Enter the AP invoice as usual and cost it to the job with the correct cost code. We recommend making a copy or scanning the invoice so you can send it to the Owner and request reimbursement. As part of the original setup, be sure the Budget does not include this cost. It should jump out at you that you have a cost and no budget. This also helps keep the responsibility with your Project Manager, since they have access to the Job Cost reports, but not the accounting reports.

When you receive the promised check, make the cash entry in the 1-2 screen. In the grid, use the same Direct Expense account that you used when the AP invoice was created. When you save, you'll get the Job Cost screen, where you'll enter the same cost code, as well.

In the Job cost details, you'll have the history of the original expense and the reimbursement for a net of zero cost to you. - *CMW*

Going From Two to One Monitor with S100C

Historically, Sage has never solved this problem. You have two monitors, use them both, then shut down. You pull out your laptop or go home to a one-monitor situation, and now you can't see the look up screen, but when you hover over the tool bar, you can see the screen is out there somewhere! It thinks there's a second monitor.

There are a couple of ways to 'fix' this, but the problem will come back when the same circumstances come up again. Our tech team has an idea—they're developing a script for our hosted clients that will make an adjustment to the file where Sage keeps track of the screen usage. We're testing it right now, so as soon as it's ready for prime-time, we'll roll it out to our hosted clients. Stay tuned! - *CMW*

Emailing Direct Deposit from S100C

Over the last several months, more and more of our clients are receiving error messages when emailing their direct deposit file, and that wasn't true before, so what changed?

Microsoft has made some updates to Office and M365 Office, adding size limits and time-outs that are interfering with the Sage 100 Contractor email settings that have worked in the past. Sage has a KB (Knowledge Base) article with some pretty odd work arounds.

For now, give us a call and we'll make the Sage-recommended changes. We can only hope that Sage addresses this in a future release, since it's unlikely Microsoft will make changes. - *CMW*

An incredible tool.

'Syscon's Cost to Complete program uses your staff's knowledge of what's happening on the job NOW to calculate where you are headed. … It seamlessly pulls in your job data with absolute accuracy … we've found it an incredible tool for many reasons, and I believe you will, too.'

-Lisa Newbold, CFO and Controller, Leff Construction.

Joke of the Month

What music do builders love?

The Carpenters.

M365 Education Station

What is Zero Trust?

Zero Trust is the principle of maintaining strict access controls and not trusting anyone, by default, not even those inside the network. Basically, Zero Trust assumes that no document, link, email, or other data source is trustworthy or safe to open.

There are 3 Key Components:
1. User/Application Authentication
2. Device Authentication
3. Trust

This approach assumes each request is from a threat. Users have multiple devices in multiple locations, not all of which are owned or managed by the company. Since you can't lock down the devices, the focus is on the user or application authentication, and security policies for the data.

For instance, Microsoft security allows a user to access files they need, but can block downloading the data to a device. As an example, in our F.I.T. System, the cell phone can see the job list and cost codes, but none of the data ends up on the cell phone.

The few things we've shared here are the tip of the iceberg. Azure Active Directory, security configurations with automation through Blueprints, sign-in with Conditional Access, MDM, and various forms of authentication all work together to make the user and/or device prove they are who they say they are. Then there's monitoring and refining of policies.

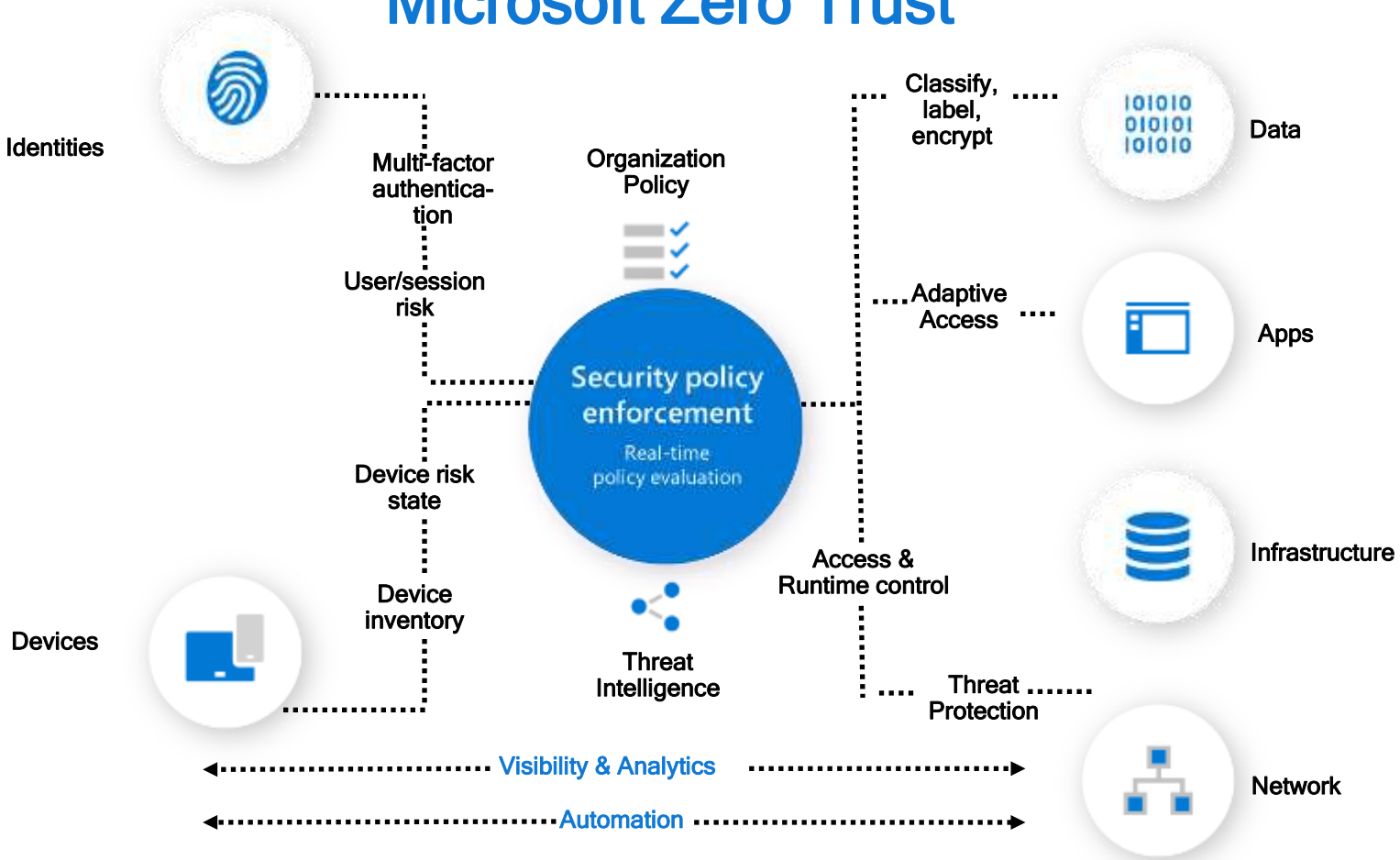
Users can find these measures very difficult when trying to work, so phasing in the changes is key to a successful rollout.

Tip of the Month

Did you know?

Azure Active Directory manages users, service accounts, and devices. User sign-in to any device can be configured with conditional access. This includes permissions and the ability to enforce them, even when accessing data in cloud environments outside your network. With M365 licenses, users can sign-in and have MFA on up to 5 devices, securely, even if you don't own them all.

Microsoft Zero Trust



How Did They Do It? Harling, Inc.

The midst of a global pandemic may sound like a strange time to purchase a masonry company, but that's just what Pat and Julie Brenner did. Pat brought his masonry experience to the table and Julie brought her accounting experience. Pat started in masonry as a teen—his summer job grew into a career. He had also worked with the prior owner of Harling to grow the business from its founding days, so they seized on the opportunity to run the company.

Harling was able to help people maintain their buildings as the early months of the pandemic played out, giving people one less thing to worry about during challenging times. What makes Harling successful? Part of it stems from treating their employees like family members, and a lot of it is their approach—they don't try to sell anything; rather, they help people with problems. Harling has four pillars: safety, integrity, quality, and customer service. Those pillars, combined with caring about and for the people who work there, are the recipe for success. Pat said he's been inspired watching the way Disney runs its company. The groundskeeper who sweeps up the popcorn at the park has many interactions with the customers, so Disney is highly selective when filling that role. Pat looks for ways to treat his people and his clients with that high level of care.

Pat and Julie Brenner, Co-owners

He said he has also been on the receiving end of care from Syscon. When they first bought the company, they had a lot of questions. Both Pat and Julie said they appreciated consulting with Cathy and Mary to help get their business running on the right foot. *-BK*

Fast Facts

Location: Westchester, IL
Specialty: Masonry
Founded: 2013
Other: Pat is a Catholic church deacon

Read more at www.syscon-inc.com/how-did-they-do-it

Are you interested in having your story featured? Let's talk!

Upcoming Events

Event: How and Why to Replace Paper Timesheets with Mobile Devices, webinar

Date: Thursday, June 17

Time: 1 p.m. CST

Register: www.syscon-inc.com/events

Recorded Webinar: Ditch the Old Server, webinar

Date: On Demand

Time: On Demand

Register: https://youtu.be/adu_Znu5SQg

Featured Articles

Business Ledger newspaper: *Security – Adding and Removing Staff*

TUG membership magazine: *What You Need to Know About Field Time Collection*

CFMA member forum, Café Connection: *Microsoft 365 Tour*

Construction Business Owners, magazine: *Finding a Home for New Software Without Replacing Your Network*

Proud Members

ASA CHICAGO

CFMA CONSTRUCTION FINANCIAL MANAGEMENT ASSOCIATION

Hinsdale SHOP • DINE • DISCOVER CHAMBER of COMMERCE

TUG POWER TO THE USER

Proud Partners

Microsoft

datto

sage

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

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