Syscon U

What's New

We're headed to Denver Colorado (actually Aurora)! This year's August State of the Company celebrates our 40th year in business, so the whole team will travel to Denver for this year's presentation and celebration events! Look forward to seeing everyone in person!

Advanced Security! This summer, we've sent a series of email messages about the importance of adding Advanced Security to your computers and Microsoft accounts. Between the bad actors and their non-stop creative attacks and the addition of AI to make things harder to detect, Advanced Security has become as foundational as anti-virus and anti-spam many years ago. Read more in this month's newsletter! - *Catherine Wendt*

In this Issue

August 2026

Identity Security: The New Security Frontier

The way we secure businesses has fundamentally changed. Not long ago, security strategies focused on protecting the network—firewalls, on-premise servers, and tightly controlled office environments, often referred to as a 'castle and moat.' But with the rapid adoption of cloud services, remote work, and mobile access, the traditional network permiter has all but disappeared. What remains at the center of your organization's security is something far more critical: identity.

Every employee login now acts as a gateway into your business. Whether it's accessing email, collaborating in Teams, opening files in SharePoint, or connecting to business applications, nearly everything depends on a single set of credentials. This shift has not gone unnoticed by cybercriminals. In fact, bad actors have adapted quickly. They no longer need to 'break in' through complex technical exploits. Instead, they simply log in using stolen or compromised credentials, often very inexpensive on the Dark Web.

Identity security has become THE number one Priority! The majority of cyber attacks now begin with compromised login information. Phishing emails, password spraying, and social engineering tactics are designed to trick users into revealing their credentials or approving fraudulent login attempts. Once an attacker gains access to a user account, they often appear indistinguishable from a legitimate employee. Traditional security tools, which were built to detect external threats, may not recognize anything suspicious at all!

Consider how much access a single account can provide. One compromised identity can open the door to email systems, shared files, internal commun-

Continued pg.2

(continued from page 1)

-ications, financial data, and critical line-of-business applications. What might start as a single stolen password can quickly escalate into a full-scale breach affecting the entire company.

Email compromise is one of the MOST common and costly outcomes of identity-based attacks. When an attacker gains access to a user's inbox, they can monitor conversations, impersonate employees, and initiate fraudulent transactions. These incidents often result in wire transfer fraud, vendor payment redirection, or the exposure of sensitive information. The financial and reputational damage caused by these attacks can be severe!

Another challenge is that once attackers gain access, they rarely stop at a single account. They often move laterally, seeking higher levels of access or additional systems to exploit. In some cases, they create new accounts, configure hidden mailbox rules, or register unauthorized applications. This allows them to maintain access even after passwords are changed, making detection and remediation much more difficult.

Organizations may face operational disruptions, compliance violations, and a loss of customer trust. In regulated industries, inadequate identity controls can lead to failed audits and potential legal ramifications. Ultimately, the cost of recovering from an identity-based breach is often far greater than the cost of preventing one.

Modern security measures provide effective ways to significantly reduce this risk. This starts with enforcing Multi-Factor Authentication (MFA) for all users, ensuring that a password alone is never enough to gain access. It also includes implementing conditional access policies before granting access to sensitive resources. Just as important is adding a Managed Detection and Response (MDR) solution that monitors and protects cloud accounts around the clock. Solutions such as Blackpoint Cyber (our Advanced Security offering) add another critical layer of defense by detecting suspicious behavior in Microsoft 365 and other cloud platforms, helping stop account compromise before it escalates.

Equally important is the principle of least privilege—ensuring users have only the access they need to perform their roles, and nothing more. Combined with continuous monitoring for suspicious login activity, MDR oversight for cloud identities, and the use of trusted, secure devices, these controls form the foundation of a modern identity security strategy.

The bottom line is simple: if an attacker gains control of a user's identity, they can gain control of your business. Protecting identify is no longer just an IT 'best practice.' It is a business necessity.

If you're unsure how your current identity security measures stack up, now is the perfect time to take a closer look. A proactive approach today can prevent a costly incident tomorrow; let's talk! - *MG/Copilot*

"The best way to predict the future is to create it."

- Alan Kay, Scientist

Book Nook

1776 by David McCullough

In this, our 250th year as a nation, we've seen celebrations everywhere, the release of the movie *Young Washington*, and special events and documentaries galore. This book was recommended to me by our friend Tim Goeglin and it turns out it was in our library!

The Founding Fathers put their reputation, their fortunes, and their lives (they were traitors as far as England was concerned) on the line. This book begins in October of 1775 when His Majesty King George III declared America in rebellion and resolved to crush it. Rather than just a narrative of the events, the book combines sections from letters and journals penned by the key players and participants, the shoemakers, school teachers, various rank and file officers, both the 'rebels' and the 'red coats.'

To say the odds were stacked against us is a HUGE understatement. Our key military leaders, Nathaniel Greene and Henry Knox, only knew what they had read about war, under a very young and inexperienced commander-in-chief, Washington. Money and powder were constant issues, as were the lack of experience and 'discipline' of the militia and army.

The book walks through various campaigns, some surprisingly successful, some ending in crushing withdrawal, from the perspective of various participants. There are maps to help the readers follow the critical land-grabs and difficulties navigating the coast. If you've read it before, this might be the year to re-read. If you never have, it is recommended! - *CMW*

A Traffic Notice is really a Trap!

Recently, I (Larry) received a text message claiming to be an 'Arizona Civil Traffic Notice..' It looked official and included a court seal, a judge's name, a case number, a QR code, and a warning that failure to pay could lead to a warrant, license suspension, and added fees. It was also a phishing attempt.

These scams are becoming more polished. The goal is simple: frighten you into clicking a link, scanning a QR code, or entering payment and personal information out of fear.

Here are some clues that gave this away. First, the message used pressure and urgency. Phrases like 'pay immediately,' 'issuance of a warrant,' and 'automatic suspension' are designed to create panic. Scammers want emotion to override caution.

Second, the web address was suspicious. It looked related to Arizona transportation, but it was not an address I recognized as an official payment site. Criminals often build links that look close enough to fool you at quick glance.

Third, the notice arrived by unexpected text message. If you do not remember receiving a traffic citation, a demand for payment by text should raise concern. Courts and government agencies may communicate electronically in some circumstances, but an unsolicited message demanding immediate payment deserves verification outside of the message.

Fourth, the message encouraged use of the QR code. QR codes can hide the actual destination until after you scan them, which makes them useful to bad actors.

So, what should you do? Do NOT click the link. Do NOT scan the QR code, and do NOT reply. Instead, independently research for the official agency or court website, or call a known, published phone number and ask if there is a citation or case associated with you. When in doubt, slow down. A legitimate organization will still be legitimate after you take a few minutes to verify it. A phishing scam depends on you acting before you have time to think or check. *–LAW*

More Texting Woah's

One of our clients received a text message from what looked like the bank, asking the client for credentials. Unfortunately, they took the bait and the bad actors hacked into the client's computer. From there, they logged into the bank and tried to make and verify a fraudulent transaction. The bad actors were actually on their computer while they were logged into the bank.

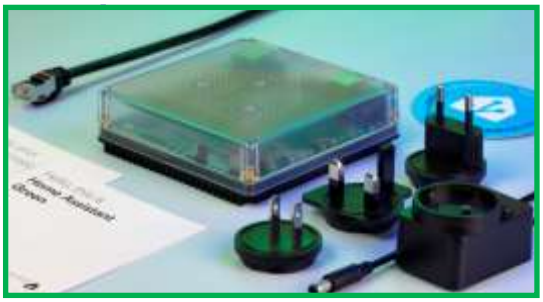
The bank took quite a hard stance, insisting that the computer be completely wiped before they would restore electronic access to the client.

As we got involved, we took this even further, checking several of our security tools, the users' Microsoft accounts, and more, locking everything down.

With all these tools in place, how did this happen? Well, when the bad actors start with a text, that goes around all the computer-specific security and they know it! Also, once you provide the credentials, not much can be done. It's like installing bars on the windows, a security system, but leaving the keys in the front door!

Banks will not ask you for your credentials; we will not ask you for your credentials; you should not share your credentials. And those QR codes, you cannot tell where they lead! Do NOT take the bait. Never provide bank credentials or even your Microsoft credentials to anyone. Not sure? Give us a call!!! *-CMW*

Shiny New Gadget Of The Month:



Home Assistant Green

Do you have smart bulbs, smart switches, smart blinds, smart speakers, and more, with a ton of apps to manage? You might want to check out Home Assistant Green.

This is an official ready-to-use plug-and-play smart home hub with Home Assistant already installed. According to their website, when the device arrives, plug in power and network cables, then download the mobile app or use the web app to guide you through the setup process. It will automatically start detecting your smart home devices. They have quite a few testimonials on their website, www.home-assistant.io/green.

The goal is to be able to control and automate everything in your home from a single app. At $199 MSRP, it has a 1.8 GHz quad-core ARM processor, 4 GB of RAM, 32 GB EMMC Storage in a translucent enclosure with an optional battery. There are two USB 2.0 ports, a Gigabit ethernet port, and large aluminum heatsink for noiseless CPU cooling (no fan!). It's pretty compact at 4.4" L, 4.4" W, and 1.3" high, weighing 12 oz.

Your data is private and local and you'll have access even when the internet is down! - *CMW*

Construction Corner

S100C v2026.2—What's New?

We've reviewed the release notes and installed the latest version in our own environment. Here's what we've learned so far and what you can expect with this latest release.

I'll start with the things I noticed right away, before I read the release notes:

- When cutting AP checks, after they successfully print and check numbers are assigned, it kept bringing me to the Lien Waiver screen! At first I thought I had just clicked something odd, but it continued. Turns out there's a new check box in the 4-3-2 screen in the lower left that says 'Print Lien Waivers after Payment' and this defaults. If you don't want (or need) this new feature, be sure you're logged on with Admin rights, use the F7 key for security, uncheck the box, and Save!
- In the 3-6 Client screen, right under the client status and type, they've added a new field, 'Rating.' Like Client types, there are no default categories so you can make whatever you need. The intention is to have a way to flag credit worthiness and similar.
- In the 1-5 Bank Reconciliation screen, they've added a few fields right at the top of the screen under the bank account selection field. This can now display the Cutoff Date Balance (not just the current). However, if the system cannot calculate this amount, it will be left blank with a message that it is unavailable. You can choose to suppress future messages and hide the cutoff balance display (which I will do).

There are the usual warnings about compatibility with older versions of Windows and Windows Server. This release has changed the way S100C passes the Federal ID number to Aatrix. You'll need version 26.2 or later to print ROE, T5018, and T4 forms.

A few more things to note:

- Three states have payroll tax changes—Arkansas, Georgia, and Utah.
- In the 5-2-1 Employee screen, across the bottom, there's a new tab to see Vacation History. This is focused on hours, not dollars, and includes all processed payroll (status 3). The history is across payroll archive years, with no drill down to last year's records, but all the hours and dates are right there.
- In the 5-1-5 Workers Comp report, they've added the ability to filter by Compensation Code.
- For those of you using the T&M Billing module, we've always had the ability to have separate labor rate tables by job, but only one table for Equipment. With this release, they will allow job-specific Equipment rate tables; might be worth testing!
- Bank Feeds! Sage is aware that Bank Feeds do not work for some Chase Bank customers. They are 'exploring solutions.'

> *"Sage is aware that Bank Feeds do not work for some Chase Bank Customers. They're 'exploring solutions.'"*

These release notes aren't usually technical, but this one had quite a few things to be aware of, so here are a few highlights.

Sage is finally echoing our long-time recommendation which is in line with Microsoft. They say that Microsoft recommends AGAINST installing SQL Server on a Domain Controller (DC) and they do not support SQL Server on a read-only DC. They have some warnings that will pop up if you try to do this.

S100C is NOT PCI Compliant. You should not store credit card information in S100C. This has always been true and most of our clients are aware, but it's a good reminder.

If you log into the Database Admin tool, you may get a message inviting you to upgrade your SQL instance if you're on Server 2019 Express or earlier—DON'T'! Just take a screenshot. You can still continue without performing the upgrade. Then, when you're done with the task, call your IT company to discuss options and timing. No one should just install an upgrade on a server without planning. If you're in our Syscon Azure environment, all these servers are running supported versions of SQL Express! - *CMW*

Two Reminders: Vacation Hours and Pay calc Accounts

It's been a while since we mentioned these, so here are the reminders.

If you don't use the Vacation/Sick accruals to track your Vacation/Sick time, the field in the Employee screen will show negative hours as people take time off. When the hours are negative, the minus sign (-) counts as a character, so as soon as you hit –900+ hours, and that week's check would put the person at –1000 hours, their payroll record won't calculate. The field can't hold that many characters.

A while back, we had recommended that as part of your payroll close process, add a task to zero-out the vacation/sick fields if you're not using S100C to track or have Unlimited PTO.

Several versions ago, Sage defaulted to requiring an account number in the pay calc expense fields to be within the range of the category. If it's a Job expense, something in the 5000-range, etc. Many clients have circumstances that require a calc outside the designated range. Choose Options, 'Allow non-standard expense accounts' to bypass this restriction. Proceed with caution! Consider impact to Job Costs, Equipment, and Departments. - *CMW*

M365 Education Station

Microsoft Price Change July 1st (yes, last month)

We knew about the price change ahead of the July 1st effective date. For our clients, it will impact M365 Basic, Standard, M365 E3 and E5, and M365 F1 licenses. However, it will not begin until your annual renewal date. The majority of our clients will not see the increase until January. A few have renewals this Fall, so coming up soon.

This is also a chance for clients with E3 or E5 licenses to move away from the Enterprise series. Several of the restrictions on Business Premium licenses compared to E3 have changed, making Business Premium a viable option and a more cost effective choice!

Become an Expert (or look like one)!

We took Chris's two-part webinar and pulled out the very practical tips and tricks, then packaged them in short segments, available on our website. Check it out!

Microsoft Solutions Partner

How Did They Do It?

Capitol Construction Services

Started in 1998 with Terry Clark and John Robinson, their partnership was primarily focused on Tenant Improvement. Their clients were often in a mall; a store closed, a new one moves in, and they remodel. This included offices and stores and they still do this type of work.

The company has grown over the years, both in its ownership as well as the type of work performed. They've added ground-up construction, primarily commercial, and have become a major supplier to a lot of Starbucks stores. They are licensed in 47 states with offices in Indiana, Tennessee, and Chicago.

There are several different entities based on ownership and responsibilities, which is part of the reason Brad was brought on board. His specialty is large data and he's built some wonderful tools to pull data and compile for presentation to the various owners, across entities, reducing the closing time to about six days, reporting to leadership by the 15th. This has allowed for transparency and integrity in the data, all presented with a PowerPoint to highlight issues and 'wins.'

When asked about their success, Brad did not hesitate; relationships! All the team members are involved, transparent, open, and honest. If there's an issue on a job, they let the customer know right away. This has resulted in long-term relationships. They focus on making sure contract changes are done right away.

Brad Goad, Controller

When asked about the biggest struggle over the last year, Brad said the cost of materials. With the tariffs, cost increases have meant closer attention and modifications to WIP schedules to reduce expected margin. Also, finding the right people.

Brad's favorite Syscon resource? After being down for six days with their local servers, the move to the Syscon cloud has been 'tremendous.' They haven't been down at all!

In keeping focus on relationships, they are also very involved with Big Brothers, Big Sisters, including sponsorship and the local board, as well as business development groups and Chambers. - *CMW*

Fast Facts
Location: Fishers IN, Headquarters
Specialty: Development, Construction
Founded: 1998
Affiliations: Big Brothers, Big Sisters

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

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

WIP Management (webinar)

When: Wed Aug 5th

Time: 11:00 am Central

A hot topic for all our clients! We'll use Acumatica Construction to show some features. No matter what ERP you use, this will be informative!

Measure Twice, Code Once: Custom Software That Pays for Itself (webinar)

When: Thurs Aug 13th

Time: 11:00 am Central

We're digging into the third Pillar from Chris's March webinar. Modern Tools are game changers!

Proud Members

CONSTRUCTION FINANCIAL MANAGEMENT ASSOCIATION

AMERICAN SUBCONTRACTORS ASSOCIATION ARIZONA

TUG POWER TO THE USER

Proud Partners

Microsoft Solutions Partner

datto

Acumatica Partner

Sage Partner

certified WBENC WOMEN'S BUSINESS ENTERPRISE

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.