Syscon U

What's New

Last month was pretty busy—attended the Global Leadership Summit; had our company-wide State of the Company presentation and dinner; attended the C12 forum in California; and spent a Saturday afternoon with some High School band friends.

With the summer behind us and kids back in school, we have one more long weekend for grilling, Labor Day. Hope you have a chance to enjoy with family and friends.

This month we're rolling out some new employee benefits at Syscon. Then it's 'nose to the grindstone' to move the rest of our Classic hosting clients to Azure hosting as we wrap up the third quarter of 2022.

- Catherine Wendt

In this Issue

September 2022

Ciphers 100 Years Ago and Today

It's hard to know if Homeland Security is doing its job or not. There's no way to know what attempts have been thwarted, what kind of monitoring is going on, and what deterrents they have put in place to take the momentum out of the would-be hackers.

There's also no question that there are bad actors out there and they're meeting with some success. Just look at how much email is blocked by spam filters, then how much still makes it to your junk folder! Turn on the news and you'll hear the stats on ransomware, warnings about scams that target our most vulnerable populations, not to mention companies, utilities, and government agencies that have been compromised, some of which have paid huge sums to retrieve their data.

Some of these 'enterprises' are run like any business with a work force, incentives for success, and to make a profit! Others seem to be state-run or at least state-sanctioned. I've heard this 'industry' referred to as the new mafia. On any front, it's big money! They're patient, persistent, and they know human nature, feeding on people's fears, taking advantage of the naïve, and doing their homework when going after a target.

In our computer-driven society, data encryption is absolutely critical. Companies such as Google and Microsoft have 'forced' us (you and me) to use encrypted communications. One example is the SSL (Secure Sockets Layer) certificates for your website. This important protocol allows for the authentication, encryption, and decryption of data sent over the

Continued pg.2

(continued from page 1)

internet. I can't tell you how many prospects' websites I visit that kick out a warning that the site is not safe because the search engine has flagged them for not having this important encryption safeguard. Even insurance companies are 'encouraging' Multi-Factor Authentication (MFA) and Endpoint Detection and Response (EDR) to renew insurance policies. In fact, there are clauses in these policies that if you have not provided the basic computer maintenance with updated patches and AV/EDR and they're compromised, they can deny your claim!

Encrypting information is nothing new, but the Enigma machine that came out in the early 1900's was a game-changer, almost the first computers in many ways. It ran on a battery, the keys were backlit, there were drums that rotated to create the encryptions, and a plugboard, similar to the old receptionist phone boards. This month's Book (below) has some great pictures and diagrams of models used during World War II. There was a Commercial model and a War model, the latter of which brought encryption/decryption to new heights.

Think back several years and you'll remember passwords were four digits, then six, then eight with mixed alpha/numeric/character requirements. When Remote Desktop connections were first available, in addition to passwords, VPN's and port number assignments were added for a second security protocol. Banks were on top of this at least two decades ago when they issued fobs which were a secondary authentication method. More recently the addition of MFA to log into email, websites, and our hosting environments, further chaining us to our phones, BTW.

Guess what helped break some of the Enigma cipher codes? Human error! Yup, the number one reason hackers are successful right now is the same reason the code breakers had success a hundred years ago! In addition to choosing the order of the Enigma drums, the operators had protocols for the actual formation of the message. The operator was to enter a combination of three letters at the beginning of the message. They would enter 'aaa' for example; then when repeated letters were found to help the code breakers, they were supposed to use random letters, so they entered combinations of letters that are next to each other on the keyboard, forward, backward, on the diagonal, but all testable and predictable patterns. This should have you thinking about all the warnings you hear about not using '123' or iterations of common words such as 'p@ssword' or anything obvious.

Let's wrap this up—the need to secure data has been part of the human condition all along. Those who study human behavior have used that for good and bad (I'd even say evil!) which is social engineering. The German arrogance that the wartime Enigma ciphers could not be broken led to a lack of diligence and ultimately the Allies' ability to read the German communications.

Our safety is on the line—the safety of our country, our communities, our family, our money, and our livelihood which is our businesses. The need for security is not new, but the methods have changed, dare I say matured, and we (YOU) need to be diligent - *CMW*

"It always seems impossible until it's done."

— Nelson Mandela

Book Nook

Enigma by Wladyslaw Kozaczuk

This book was written in 1984 and is one of several on the topic of the Enigma encryption machines used during World War II. As I read the book, I was constantly reminded of things happening right here and now in 2022.

The story focuses on the contribution of a Polish cryptology department and three amazing mathematicians, Marian Rejewski, Jerry Rozyck, and Henryk Warsaw under some excellent leadership, all of which was kept very secret for good reasons! All these years later, the author is shining the light and putting the record straight on the significant Polish contributions in decrypting German communications.

There were other countries working on cryptology, even prior to World War II. This team eventually shared their hacking successes with England and France. Throughout the war, the Germans continued to change the cipher process in various ways, but each time, these teams tackled the new challenge. Decrypting these messages was absolutely critical to the success and subsequent victory of the Allied forces.

The layout is well researched and truly conveys the successes, failures, and the personal risks and sacrifices this team and many others made. It also highlights the arrogance of the Nazi party since they thought the encryptions could not be decrypted, but they were wrong. In addition to the story of these men, this special program, and the historical timeline, there are many pictures and articles; Highly Recommended! - *CMW*

Basic Auth—End of Life

Many of our clients use Basic Authentication (referred to as 'Basic Auth') for SMTP email which is used for Direct Deposit and ACH email notifications. Microsoft has been very clear that it considers this service a security risk, so on October 1st, they're turning it off.

Any software programs that use SMTP to email notifications (and Sage 100 Contractor is one of them) will need a replacement option. In general, the SMTP protocol circumvents the Multi-Factor Authentication (MFA), an important security safeguard that is actually required for many insurance renewals (and we strongly recommend it, too).

The clock is ticking on this, so if you're not sure if your scan to email is using the SMTP protocol, it's time to ask some questions. If you're a Sage 100 Contractor user, version 24 supports the replacement authentication; a good reason to upgrade if you haven't already.

If we manage your email, give us a call. We'd like to setup the replacement option prior to October 1st so it can be tested without any work interruptions. If someone else handles your email, be sure to reach out to them right away. We're happy to assist, as needed, of course! - *CMW*

Windows 11

Hard to believe Windows 7, a very popular operating system, was end-of-life in January 2020. Everyone had to be on Windows 10 and for many of our clients, that meant replacing hardware, as well.

In October 2021, Windows 11 was released. As is often the case, not all business software is compatible with new releases, but as we watched this roll out, we saw very few issues. There are some changes to the Start menu and a Mac-like design along with a beautiful background screen!

Most of our techs have been running Windows 11 for several months (or more). Beginning now, all new computers that we quote and order for you will have Windows 11 as the operating system. — *CMW*

Network Solutions—Back on our 'Naughty' List

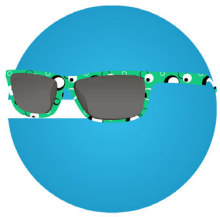
We have a client story to share: They called because they noticed they weren't receiving any inbound email, and when they checked, their outbound email wasn't being received by the recipient.

The techs dug in and noticed that all email flow reports were showing the messages as delivered, and outbound as having been sent; odd. Digging in a little further, turns out 90% of all inbound messages were being marked as High Probability Phishing and were automatically moved to the quarantine folder, which is why they couldn't see them.

When the techs checked the message headers on the 'spam' email, the DKIM signatures were missing from the email headers even though DKIM was configured for the client's domain.

Since DKIM is enabled and configured through DNS (Domain Name System), the issue had to lie within the DNS servers, which are hosted by Network Solutions for this client!

This isn't our first DNS problem with Network Solutions (see May 2022 newsletter) so we weren't going to play around. The techs migrated DNS to Cloudflare which resolved the DKIM signature issue within 10 minutes! - *CMW*



Shiny New Gadget Of The Month:

Ekster Parliament Wallet

This wallet is a premium leather smart wallet designed for slim storage and quick card access. The built-in aluminum cardholder fans out your cards at the click of a button and protects them against skimming. And a tracker card makes it 'unlosable' according to the website.

Features include a patented quick card access mechanism, RFID blocking technology, environmentally certified leather, and a tracker.

It's 0.4 x 4.1 x 2.5 inches, has a cash strap, and stores up to 12 cards but they recommend keeping it to 9. The wallet is $89 with the optional Tracker Card for another $49, but there was a sale on the Ekster website (not sure how long it runs).

These seem to be targeted for the men in our lives. Simple design, quality components, easy card access and a slim layout. Check it out at ekster.com. Too early to think about Christmas presents?

CONSTRUCTION CORNER

Equipment Module—Indirect Costs

We've seen a renewed interest in tracking indirect costs, sometimes focused on owned equipment, other times focused on the cost of running a shop and keeping equipment in good repair. The Equipment Module in Sage 100 Contractor is pretty powerful. Some clients are only using it to track equipment and shop costs; others are using it to show equipment costs on specific jobs; others have large equipment and use it to track and post amortization and finances. Let's take a look at how some of this works.

The two primary drivers are a specific General Ledger account range which isolates these costs from job-specific costs, as well as true overhead costs, and the equipment itself. In this Indirect range, we have an opportunity to capture costs that indirectly support the contract field work. This could include shop labor and related expenses; fuel costs; shop supplies; safety equipment, shop rent, cell phones and other equipment used by project managers and shop staff; field-related vehicle maintenance, repairs, and fees; the costs to maintain and repair company-owned equipment; and similar items.

The pieces of equipment can be general or specific. Some clients have a piece of equipment called 'Trucks' and track all truck-related expenses to this group. Others have each truck as its own piece of equipment to help watch the expenses and balance maintaining something old with replacing it. There's usually one piece of 'equipment' called Shop to collect time. This could be for a shop manager, or to track hours spent 'sweeping' the shop and general tasks. If you're tracking specific equipment, a mechanic can actually break down their time by which piece of equipment they were working on so you can track labor as well as outside costs.

> ***"Now you can run reports of costs for specific pieces of equipment and for the shop. It can be pretty eye-opening."***

Similar to the Direct Expense range, when you use the Equipment/Shop range of the General Ledger numbers, you get a second costing screen. Instead of a list of jobs, you'll see a list of equipment. Choose the Shop or the '#5 truck' for example, then add a brief description, cost code, cost type, and dollar amount. These create cost records that are now associated with the selected equipment/shop.

In Payroll, rather than choosing which job, you choose which piece of equipment or the Shop for the person's time, then add a cost code. Choose a job and their time will be costed to the job; choose the Shop or a piece of equipment, the costs will go there; leave these two fields blank and their time will to go overhead.

Now you can run reports of costs for specific pieces of equipment and for the shop. It's pretty eye-opening to see how much time is spent and how many dollars are spent in support of the field work. If you didn't have any jobs, you wouldn't need someone in the shop, fixing equipment, loading the trucks, and so on. On the financial reports, you can now see direct job costs separate from supporting shop work. You'll see the income minus the direct job costs, then the indirect costs. Do your job markups correctly reflect what it costs to cover these indirect expenses?

For specific equipment, you can track serial numbers, date of purchase, license plate info, and other info. There's even a tab to determine cost recovery rates. If you have heavy equipment, you can also track a lot of information about original capitalization, depreciation, and financing.

Another amazing feature of this module is the ability to charge a piece of company-owned equipment to a job at a recovery rate. Options include a dollar amount per day or per hour, operating and idle time. When this is setup and entered correctly, it creates job cost records that can be included in T&M Billing and also better reflects the true cost of the job—if you didn't own it, you'd have to rent it!

This is a separate module and may need to be purchased. Next month we'll talk about several things that need to be setup and considered when implementing this module.—*CMW*

IL State Mandate Beginning November 1st

Companies with 5+ IL-based employees, in business at least 2 years, must offer their own retirement program or facilitate the state retirement program, Illinois Secure Choice. The deadlines are staggered based on number of EEs—insane!

S100C v24 and Printing Payroll

Mary stumbled on this one, then a client called, too. If you use Direct Deposit and then have to write a manual check, you have to delete your default report settings in order to print a check.

Even if you choose report 21 instead of 22, it will not allow you to print the paper check. There's a knowledge base article on this from Sage if you want to check it out.

In the upper left corner, choose Defaults, then 'Delete Printing Defaults.' Choose report 21 and follow the steps to print the check. Reset your defaults for Direct Deposit and this problem won't come back! -*CMW*

M365 Education Station

4 Ways to Secure M365

Microsoft works to keep your company's data secure, but you have a role to play, too. Here are four (4) things you can do to help keep your company's data safe:

1. Set Up MFA!!

Multi-Factor Authentication (MFA) requires more than just a user name and password. Another source of verification is required such as a special code to your phone for additional confirmation.

2. Train Your Users

Educate, continuously! Require MFA; provide reminders to not click links; never provide a password in response to an email request; never send a user name and password in the same email.

3. Classify Data

Classifying your data into distinct categories and groups allows you to apply custom controls such as policies and file restrictions. This might include limiting access, restricting the ability to share files or even download to a local device.

4. Adopt Zero Trust

Zero Trust is an approach that begins with the premise that nothing is trusted and all interactions have to be confirmed first. It assumes no document, link, email, or other data is safe to open.

Microsoft deploys some sophisticated artificial intelligence (AI) to stop cyber attacks. More specifically, Microsoft uses machine learning, which is a type of AI. Without human intervention, Machine Learning (ML) uses historical data to make predictions about what is safe. In other words, ML is a smart type of AI that teaches itself to recognize possible cyber threats and stop them before they cause harm.

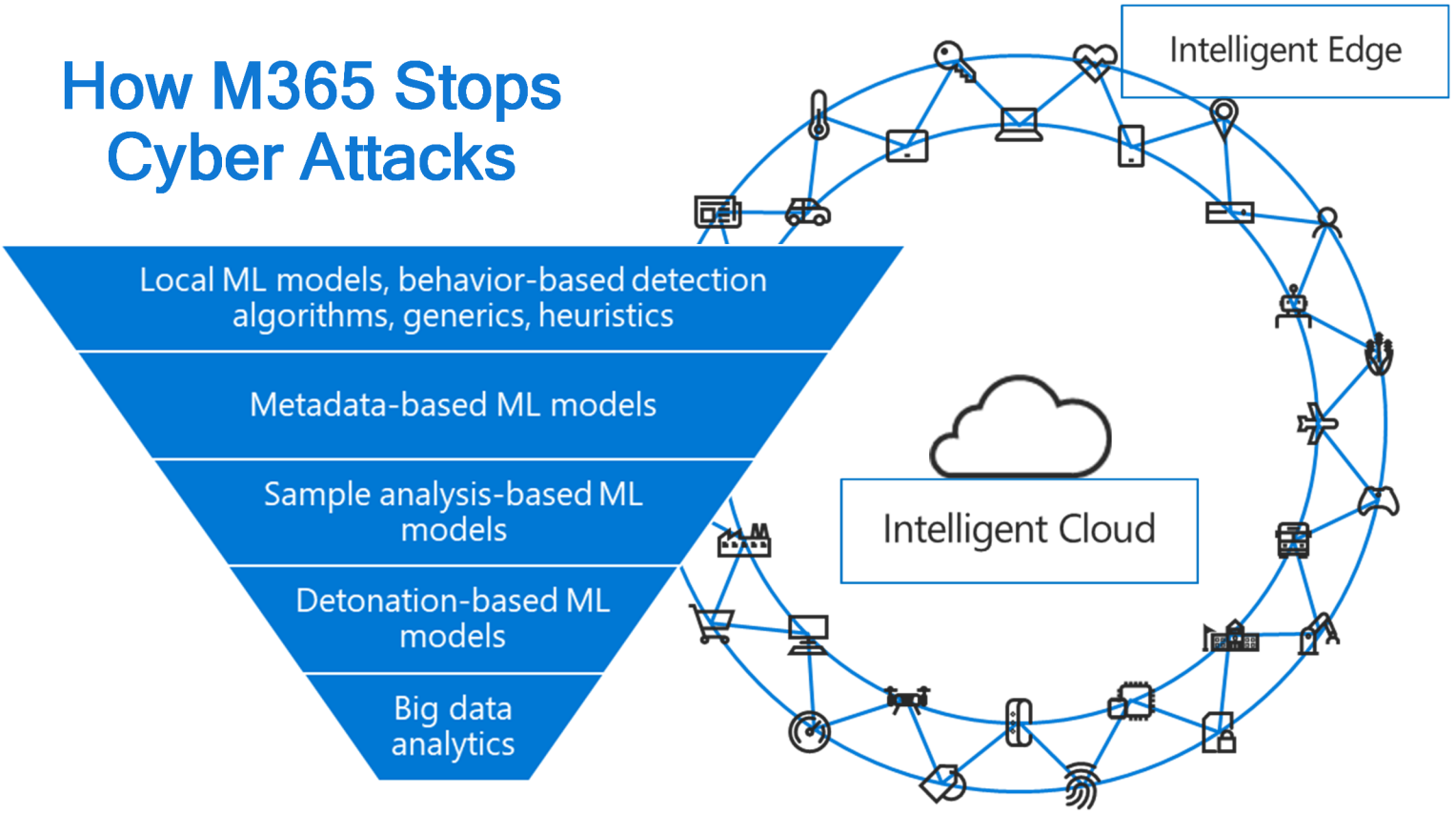
Tip of the Month

Did you know?

M365 Business Premium licenses (and higher) have the option to encrypt your email. From the Option tab, you can choose protection options such as encrypting email before you send, and even disabling the ability to forward your email.

These additional security options are built in to several M365 license levels. If you send sensitive numbers or other sensitive info via email, we strongly recommend you move up to one of these license levels!

How M365 Stops Cyber Attacks



Microsoft | Partner

How Did They Do It?
Precision Excavation

"Complacency will be the architecture of your downfall." – Jeremy Gutsche

Before COVID hit, the phones at Precision Excavation were practically ringing off the hook. There was no shortage of work in the commercial sector. The company was focused on keeping their customers happy; this approach generated a lot of referrals. During the worst of COVID (and after), uncertainty took hold. Customers didn't know where the market was going. Precision Excavation faced supply issues and customer work was put on hold. They needed a new game plan.

They diversified – they hired an estimator with relationships and experience in the suburbs. This generated new business. "We learned we can't be complacent. When we're busy, we need to continue to think of ways to improve and continue to look for new business, even if we don't think we can take it on," said Controller Angie Dillon.

Angela Dillon, Owner, COO

Precision Excavation also looked for ways to increase their efficiency. Angie manages the company's finances, payroll, insurance, and vehicles. Using Sage 100 Contractor for certified payroll saves her a lot of time. The project management tools in Sage make it easier to help Angie determine how much they spent on a job. "It's so much easier than having to do it manually. Everything has run pretty smoothly," Angie said. *—BK/CMW*

Fast Facts

Location: Chicago, IL
Specialty: Excavating, Demolition, Soil Retention
Founded: 2004

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: Field Time Collection the Easy Way, webinar

Date: Thursday, Sept 15th

Time: 1:00 p.m. Central

Register: www.syscon-inc.com/events

2022-2023 Theme

Team Momentum

Who We are

How We Work

Proud Members

ASA CHICAGO

CONSTRUCTION FINANCIAL MANAGEMENT ASSOCIATION
CFMA

Hinsdale SHOP • DINE • DISCOVER CHAMBER of COMMERCE

TUG POWER TO THE USER

Proud Partners

Microsoft

datto

sage

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.