Syscon U

What's New

Great event in Atlanta, the CFMA Annual Conference. Hundreds of construction financial professionals gathered to learn and to share. Lots of great speakers and Chris did a great job presenting Power BI in a break out session!

This month we honor our fathers and the men who have supported, nurtured, encouraged, and challenged us throughout our lives. We also have quite a few graduations in the Wendt-Aikman family. So exciting to see these young people opening new life chapters!

If you haven't met Liz yet, you will soon! We are excited to welcome Liz in her new role as our IT Coordinator.

- Catherine Wendt

In this Issue

June 2022

Cyber

:of, relating to, or involving computers or computer networks (such as the Internet)

Security

1. The state of being free from danger or threat
2. Freedom from harm, physical or psychological
3. Freedom from fear or anxiety
4. Protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries

Cyber Security — Controls To Have In Place

This is a HOT topic! We held a webinar with cyber insurance experts; there were several breakout sessions at the recent CFMA conference; and we presented to four (4) local Chambers during a lunch event focused on cyber.

This is when quite a few business owners tune out! They think they're too small and this doesn't apply; that could not be further from the truth! This is a numbers game and it's worth a fortune. The big companies may be a bigger pay out, but it takes longer and a lot more effort and planning, more resources. Smaller companies are less secure and there are so many of them that the odds of success are quite high. YOU are their EXACT target. *MSP Success* magazine reports that 43% of cyber attacks in 2021 were against small businesses. Roughly 60% go out of business in six (6) months following a cyber attack, according to the same

report. Kind of sobering, so keep reading...

There are some physical and some 'soft' components to cyber security. The physical components include the server (on premise and hosted), firewall, wi-fi, routers and switches, laptops/workstations, tablets, and phones. For many of us, backups are also physical (although there should be an off-site component, as well).

'Soft' components include log on credentials, email, SaaS (Software as a Service) applications, Contact Relationship Management (CRM) software, remote access solutions, documents and files, financial software, industry-specific software, internet service (ISP), anti-virus and anti-spam. Insurance, domain hosts, and backups can be added to this

(continued from page 1)

category as well. Each of these items have their own considerations and we have stories! For now, we'll focus on some questions for you and your team. It's important to know what you have to protect, what is at the highest risk, and what controls you can confirm or can begin rolling out to move forward. It's important to know that this is not a 'one and done' task. This needs to be a regular topic with a budget and someone who 'owns' the project.

So what data is where? Here's a list to get you started: ACH bank info for clients and vendors; client data including contacts and financial history; client credit card numbers; company credit information; log on credentials for banks, utilities, and critical software; drawings/blueprints of public buildings; employee direct deposit info and other personal info such as Social Security numbers; new hire forms; and so on.

Where is this data? Do you have thumb drives or external hard drives? Where are they? What kind of data is on them? Think about the data list you just made; do any employees have copies on local computers or home computers? Maybe you use Drop Box or SharePoint; do you have security in place and are these backed up?

Where are your backups? Have they been tested lately? Years ago, testing tape backups was a pain. Current backup solutions are much easier to test. Many in our industry suggest the 3-2-1 rule; 3 copies, 2 off-site, 1 onsite. Image-based backups are the standard and encryption in transit is a must. A true disaster recovery solution allows you to mount a server image locally or in a secure cloud.

Consider the types of risk: Human (#1, BTW), Natural, Technical, and Environmental. Here's a 'fun' game—run through some scenarios. If 'X' information was not available, what would be the impact to the company? Say if email went down, could we function? What if jobsite documents weren't available; the open receivable or payable list was gone; could you get payroll out? One

of our Texas clients was a victim of the odd ice storm in February 2020. The payroll service couldn't get the checks to their office and didn't know where they were. What's your backup plan? (We helped, BTW)

There's so much to cover! I'll leave you with eleven controls to reduce risk as shared at the CFMA conference, a place to start. 1) Patching; 2) Know your data; 3) Stay current with technology; 4) Training; 5) Anti-Virus/EDR; 6) Monitoring; 7) Password & Encryption; 8) Data backups; 9) Control Admins (should be minimal); 10) Manage Vendor Risks; 11) Cyber Insurance. Lots to consider; we're here to help! - *CMW*

> *"Your time is limited, so don't waste it living someone else's life."* - Steve Jobs

Book Nook

The Customer Service Revolution
by John R. DiJulius III

I heard John DiJulius speak at a recent industry event in Nashville. His passion for the Customer Service revolution is sincere and compelling.

Whether it's in-person customer service, a call center, or online, people's expectations are moving away from purely transactional to relational. When it's just a transaction, we tend to move to price. If it's a relationship, a positive interaction, price can move lower on the list.
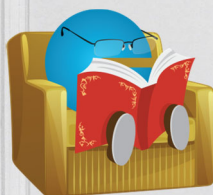
There are many examples of how simple word changes to contracts, signage, and other communication can change how we come off to prospects and customers. He has so many examples, you'll want to read them through.

Not all of our staff members are wired to be in customer service rolls, so hiring is still very important. Even those who have great 'raw materials' still need training. He makes strong arguments to train and retrain to hold the standards high. There's an entire section on the-day-in-the-life of a customer; what a great idea. This is an easy read with great examples and strong arguments; I have lots of notes! Definitely Recommended! -*CMW*

TECH TALK

7 Factors That Influence Phishing Risk

Phishing is the No. 1 cyberattack risk that businesses face. 84% of businesses were victims of a successful phishing attack in 2021, which is a 15% increase over the same 12-month period in 2020. There are 7 factors that influence a company's phishing risk:

1. Human Error—an estimated 90% of security breaches are due to human error.
2. Social Engineering Traps—97% of employees are unable to spot sophisticated phishing emails.
3. Carelessly Handling Attachments—48% of malicious email attachments are disguised as a routine file.
4. Irregular/Non-Existent Security Awareness Training—Over 50% of businesses fail to engage in regular security awareness training.
5. Lack of Caution When Clicking Links—1 in 3 employees are likely to click links in phishing emails.
6. Weak Security Culture—56% of small business owners are not very concerned about being the victim of a cyberattack.
7. Fear of Repercussions—40% of employees don't report potential phishing for fear of getting in trouble and about 30% of employees fail to report cybersecurity mistakes out of fear.
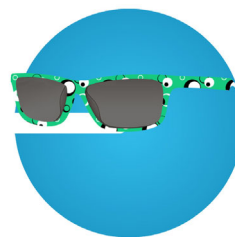*-ID Agent*

Coca-Cola Company Attack

Ransomware group Stormous claims credit for stealing 161 gigabytes of data from The Coca-Cola Company. This hacking group has been linked with Russian hackers. Financial data, passwords, and commercial account records are reported to be among the stolen data. No information about consumer or employee data exposure is available. *–ID Agent*

3 Reasons the Dark Web is a Threat

The Dark Web is a part of the Internet that is not indexed by search engines. It's not easy to navigate to and is full of illegal activities. It also presents danger to businesses. Here are 3 reasons the Dark Web poses a threat:

1. The Dark Web is Hopping—Activity on the Dark Web has grown steadily in the past 2 years. There are over 3 million active users daily, almost 10% of whom are from the U.S.
2. It's Easy to Buy & Sell Credentials—Usernames and passwords are a hot commodity on the Dark Web. Legitimate corporate network credentials sell for around $3,000 and legitimate privileged user creds can go for as much as $120,000. Credit cards with an account balance up to $5,000 go for $120; $15 can get a hacked Uber account or PayPal transfers; a DDoS attack to an unprotected website is just $45.
3. Dark Web Credential Exposure is a Gateway to Disaster—User credentials guard an organization's systems and data. When those credentials are sold and purchased on the Dark Web, a data breach or worse can happen quickly. An estimated 15 billion unique logins are circulating the Dark Web right now. *–ID Agent*

Construction Corner

Insurance—You NEED To Read This...

In April we invited our insurance agent and two Cyber Security brokers for a panel discussion webinar. It was quite lively as we dug into the changes, everything from the length of time for the application process, the demanding requirements, to the rising costs.

Then in May at the Construction Financial Managers Association (CFMA) annual conference, several of the breakout sessions focused on insurance. Here are a couple of topics you may want to dive into.

Are you working in **new states**? Many of our clients have expanded into multiple states, something that is new for them. If you are, or you're planning to, check in with your insurance agent. There may be different Workers Comp (WC) classes in the new state. At a minimum there will be new rates and you'll need to setup the additional states/classes in the Workers Comp payroll tables, both to collect data for the audit and to get the right rates in your job costs.

Some of our clients have **OCIP/CCIP** jobs where the owner or GC is covering some of the insurance. When it comes time for the audits, you'll need those CIP Certs available. Be sure you've read them and know when the third-party coverage starts and stops and exactly what insurance is being provided. You can attach these CIP Certs to the 3-5 job screen for easy retrieval, or save them to your electronic job files (they are electronic, right?).

Did you know there's a code for **Clerical Office Telecommuter, #8871**? I had no idea! If some of your work force is working remotely, you might want to check with your agent and get some rate info. Also, there are often different codes and rates for **Residential versus Commercial** work, even for the same trade/task.

> ### *"Did you know that the PPP Funds can be audited for up to six (6) years?"*

Here's a good one—there are a growing number of you that are using outside **temp agencies** to supplement your work force. At a minimum, they should provide proof they have WC and Gen Liability for the temps. Turns out they can also add you to their policy. What if one of the temp staff members is injured when they're on one of your jobs? A claim would start with the temp agency, but you may be pulled in as well. If you were named on their Certificate of Insurance, you would have a layer of protection.

With out-of-state workers, there are often **additional forms of compensation, beyond the W-2 wage**. Check your policy, check with your agent, and be sure you know what other items might be subject to Workers Comp. Things to consider are the rental value of an apartment, meals/lodging, or store certificates/gift cards you provide for incidentals.

There's a fairly new insurance coverage called **Employee Benefits Coverage**. The example is an employee gets married or needs to move to family coverage after the birth of a child. They let your HR know, but that person doesn't get the changes turned into the insurance company. Then that same employee has a claim, only to find out the coverage was never activated. Who pays the bills? This insurance is meant to fill in the gaps. I'm told it's not very common, but not expensive, either.

Do you use drones to monitor your job sites? What if one of them crashes and causes a car accident? Don't worry, there's **drone insurance**! If you're flying drones commercially and charging for the service, this is an absolute must. If you're using them for your own company, you still have risks; something to consider.—*CMW*

PPP Funds, Forgiveness, Audits

Many of you received PPP funds, tracked your allowed expenses, and provided documentation so the loans would be forgiven. At the CFMA conference, one of the breakout sessions brought up some very interesting info.

Did you know they can audit these loans for up to six (6) years? It is well known that there was fraud. The rules as to what was allowed or not kept changing as we did our best to track. Seems like this could be a target for the Feds to audit and recover some of the money.

So where do you have your audit documents? Does your owner know where they are? Are you prepared to pull them out in 5 years and have them scrutinized? Quite sobering. Might be time to revisit and get prepared. - *CMW*

Do Not Hesitate

'Do not hesitate to use Syscon as your business partner.'

-Julie Brenner, Accountant, Harling

Joke of the Month

Where's the best place to store dad jokes?

In a dad-a-base!

M365 Education Station   Microsoft | Partner

7 More Things to do in Teams

1. Make a Chat Group

Create a small group chat with colleagues you work with most closely. You can name and 'favorite' the chat for easy reference.

2. Connect From Anywhere

Download the Microsoft Teams desktop and mobile apps to enable teamwork from anywhere.

3. Find Someone's Time Zone

Hover over a person's profile picture. Under Contact, the local time for that person will display.

4. Stream Live Music

Want to set a mood to motivate coworkers/employees? Enable the High Fidelity Music Mode in the settings (Settings>Devices>High Fidelity Music Mode). Select the music note at the top of the meeting window while a meeting is in progress.

5. Pin a Message

Pin a specific message to the top of a chat so it's always visible to the members of the chat, no matter how many messages come after the pinned message. Only 1 message can be pinned at a time.

Click on the 3 dots next to a chat message and select Pin.

6. Change How Many Messages Are Visible

The default chat density is set to comfy mode. To see more text, click on Settings and More in the upper-right corner of the screen. Select Settings>General. Select the Compact chat density option.
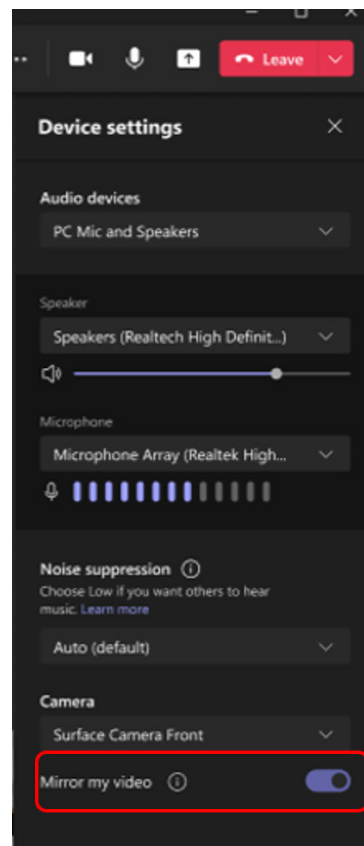
7. Turn Off Mirror My Video

Before entering a meeting, toggle the Mirror My Video off. Mirror My Video lets the user see themselves as if they are looking in a mirror. Turning Mirror My Video off lets a user see themselves the way other meeting participants see them.

Mirror My Video On:
Mirror My Video Off:
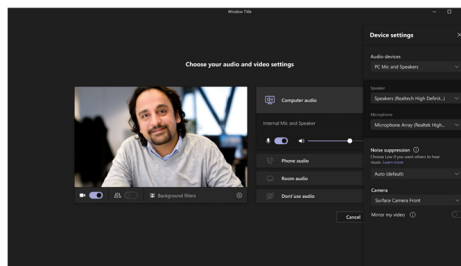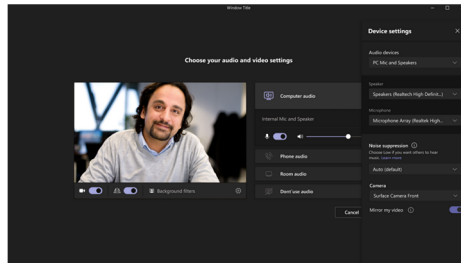
Toggle Mirror My Video On/Off:

Tip of the Month

Did you know?

It is possible to auto-record meetings. Go to Meeting Options, then toggle the Record Automatically option to 'yes' before the meeting begins. When the meeting starts, Teams will automatically begin recording.

Once the meeting ends, the video will appear in both the meeting chat and in the Microsoft Stream app.

Fun Facts About Teams
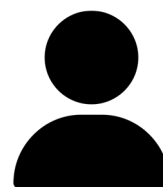
270 Million Active Monthly Users

500,000 Companies Use Teams

Launched March 14, 2017

How Did They Do It?
Weaver Brothers

Be prepared for anything and try to sleep at night. These two practices equip Adam Bates, co-owner, for success. The unexpected often interrupts a planned workday, such as a sick worker, another subcontractor running into an on-site issue, or terrible weather. Weaver Brothers got a call shortly after heavy storms washed out the sole boat launch of a state-owned lake, so there were several people with nowhere to secure their boats – all this transpired shortly before a holiday weekend. Weaver Brothers obtained an emergency permit and got working right away. They were able to rebuild the launch before the holiday weekend.

Adaptability was the key to handling this unique situation – and every other challenge that comes along to keep the business operating. Technology has become much more relevant to running the business, Adam said. Prior to implementing Syscon's Indirect Cost Allocation, Office

Manager/ Accountant Shari Courser was calculating job costs by hand and

Weaver Brothers Construction Company
Road and Earthwork Contractor
1629 Route 3A
Bow, NH 03304
Tel: (603) 228-8631
Fax: (603) 228-5375
www.wbcc.biz

in Excel. Now it's a very simple process she can do in a matter of minutes.

That frees her up to help with other projects, including the Weaver Brothers' own scholarship program. The Mark Bates Scholarship Fund was established in honor of the late Mark Bates, who started his career at Weaver Brothers at age 18 and worked his way up from laborer to co-owner (much like current co-owners Adam, Peter, Jason, and Jeff Bates). —*BK*

Fast Facts

Location: Bow, NH
Specialty: Road & Earthwork
Founded: 1946
Affiliations: Associated General Contractors of NH, NH Good Roads

(www) ***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: Take the Pain Out of Field Time Collection, webinar

Date: Thursday, June 9th

Time: 1 p.m. CST

Register: www.syscon-inc.com/events

————————

Event: Teams 101, webinar

Date: On Demand

View the Webinar: www.syscon-inc.com/microsoft-365-resources

————————

Event: Teams Getting Started, webinar

Date: On Demand

View the Webinar: www.syscon-inc.com/microsoft-365-resources

Featured Articles

TUG member magazine:

Phishing: Social Engineering, Oh My!

Daily Herald newspaper:

The Changing Face of Cyber Defense

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.