ALL THINGS TECH

Brought to you by **SYSCON**

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

What's New

December: the last month of 2019; time to order bankers boxes and W-2 forms; time to plan office parties; and time to plan equipment purchases to take advantage of the Section 179 tax incentives, just in time to beat the January 2020 Microsoft deadlines!

I'm sure you've seen our bright pink reminders on our invoices, heard our video blogs, and read our regular messages about the end-of-life for Windows 7 and Server 2008 Operating Systems. You have a little over a month to get all that equipment swapped out!

And somewhere in there, we have a lot of shopping to do!
- *Catherine Wendt*

December 2019

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.

Cybercriminals Are Taking Aim At Your Business ... Is Your Network Protected?

Cybercriminals love to test your defenses. They love to see how far they can get into the networks of businesses all over the globe. Cybercriminals really love going after small businesses because they can all too often sneak onto a network, copy data, and move on. Through the use of ransomware, they can hold your data hostage and refuse to cooperate until you pay them some amount of dollars – and if you don't pay up, they threaten to delete all your data.

But protecting yourself is not as hard as you might think. While cybercriminals and hackers are an everyday threat to businesses, you can take steps to significantly reduce that threat and take that target off your back.

The first thing you need to do is understand why cybercriminals target small businesses and what makes your particular business vulnerable. There are many things small businesses do and don't do that open them to attack and data theft. These may include not having enough (or any) security in place or not training employees on security protocols.

Realistically speaking, the biggest threat to your business does, in fact, come from your own employees. This doesn't mean they are intentionally harming your business or leaving your network exposed to outside threats. It means they don't have the proper training and knowledge to protect your business from a cyber-threat.

Continued pg.2

Get More Tips and Topics: www.Syscon-inc.com
630.850.9039

(continued from page 1)

For instance, your team needs to be trained to use strong passwords, and those passwords *must* be changed periodically (every three months is a good rule of thumb). A lot of people push back on strong, complicated passwords or use the same password for everything, but this is just asking for trouble and should not be allowed at your company.

Once strong passwords are in place, enable two-factor authentication (2FA) on everything you possibly can, from network access to every account you and your employees use. This is an additional layer of security on top of standard password protection. This feature is generally tied to a mobile number or secondary e-mail, or it may be in the form of a PIN. For example, when 2FA is enabled, after you've put in your password, you will be prompted for your PIN for the associated account. Many of us have experience with this when logging on to bank websites.

Another thing you must do to get that target off your back is to get anti-malware software installed. Every workstation or device should have some form of this protection. Not sure what to use? This is when working with a dedicated IT company can come in handy. They can help you get the right software that will meet your specific needs without slowing you down. They will install software that is compatible with your PCs and other networked equipment. Plus, they will make sure anti-malware software is working and is regularly updated.

On top of this, you want to have an active firewall in place. Every business should have its network protected by a firewall; like anti-malware software, firewall security comes with a number of different settings, and you can customize it to fit the needs of your network. Firewalls help keep attackers and malicious software off your network. When paired with a good anti-malware software, your layers of security are multiplied. The more layers, the better protected you are.

Finally, with all of this in place, your employees need to know what it all means. Keep your team up-to-date on your business's security protocols. This includes items like your password policy, malware protection policy, and proper e-mail and web-surfing etiquette. The bad guys are never going to stop attacking, but you have the power to protect your business from those attacks.

Cathy and Larry Sightings

Catherine attended a two-day industry conference in Vegas, and spent two days with a client in WI (thanks Dennis and Chris).

Larry visited a non-profit in CO to assist with a technology assessment and continues to perform with two local orchestras in the Phoenix area.

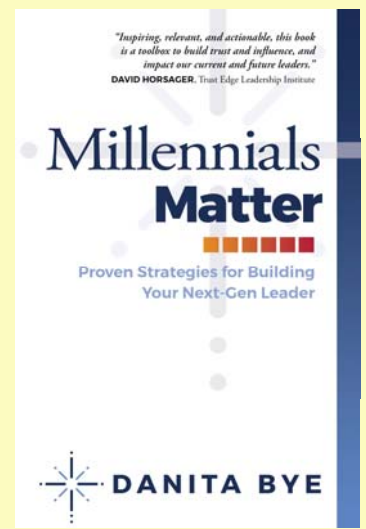*'You must welcome change as a rule but not your ruler.'*
- Denis Waitley

Millennials Matter by Danita Bye

Danita Bye held a breakout session at the C12 Currents event in GA this past May. Her background is in training sales people for success. In more recent years, she has turned her attention to training and mentoring Millennials in the work place.

Many of the stereotypes associated with the Millennials are true; Ms. Bye discusses several of these, and even includes quotes from Millennials with their take on this generation's strengths and weaknesses, how they were raised, and their choices as they enter and want to succeed in the work place.

I can't say there were 'revelations' in this book, but there were many helpful takeaways and some excellent reminders. I found myself highlighting many reminders that pertain to leadership in general. Her focus is how to share, walk alongside, not just 'teach' these great lessons when working with the Millennial generation in the work force. I found myself irritated a few times, but then remembered that it is our job to welcome, mentor, and coach our staff for success, personally and professionally. This book is definitely worth your time; bring your highlighter. - *CMW*

"Inspiring, relevant, and actionable, this book is a toolbox to build trust and influence, and impact our current and future leaders."
DAVID HORSAGER, Trust Edge Leadership Institute

Millennials Matter
Proven Strategies for Building Your Next-Gen Leader

✦ DANITA BYE

From the Techs

HD Mask Surveillance Camera USB Spy Cam

Sometimes, you don't want security cameras in plain sight or you don't even want to go to the trouble of installing cameras. Meet the HD Mask Surveillance Camera USB Spy Cam. This device makes video monitoring easier than ever.

The HD Mask is a tiny camera disguised as a USB charger. At a glance, you would have no idea it was a camera. Even better, it actually works as a USB phone charger, which really sells the disguise. It records as soon as it's activated with motion and has many practical purposes, from keeping an eye on pets to monitoring certain areas of your office for security purposes.

You can access the footage right on your smartphone and watch in real time. Learn more at HDMask.com.

Scheduled IT Work— What To Expect

We often schedule specific times to work on your computers. We might have time set aside to troubleshoot an issue, upgrade software, or setup new equipment, for example. Based on our relationship with you and our experience with the task at hand, we estimate about how long we'll need, then we schedule that time block with you.

Planning ahead helps us and it helps you; how?

- For us, we can have checklists available, other resources ready, pre-arrange licenses we might need, and we have dedicated, uninterrupted time to get the work done.
- For you, you know when to expect our call, about how much time to block, whether your office will be interrupted, what we need you to have ready, and similar items.

This allows all parties to prepare for interruptions in the workday and to be sure we have everything we need so there are no delays.

What we sometimes find is that when we call or arrive for the scheduled time, you have a short (or maybe not so short!) list of other things you're hoping to have addressed as well.

The techs don't want to let you down or say no, but honestly, the time we have blocked is only sufficient for the task at hand. We won't be able to add more items within the scheduled block of time.

There are a few options – if it's really an unexpected emergency, we can regroup, address the emergency, and reschedule the original work. If it's not an emergency, we'll ask you to choose which is the higher priority; the list you just gave us, or the task we originally planned to do that day?

BTW – we prefer to stick with the plan whenever possible since that's what we're prepared to work on. Sometimes the items on the new list require some planning or resources that may or may not be available.

We plan ahead for these scheduled tasks, whether they're onsite or remote. This helps you and it helps us. We really can't extend the time slot since we often have another commitment at the end of the blocked time. If we try to add more things, that will make us late to our next scheduled client, and that client could be you!

Any questions or if you need to do some planning, just let us know. – *CMW*

*A **very** intense 3-day training event with Darren Hardy and his A-Team in La Jolla CA.*

Construction Corner

Indirect Cost Allocations Part II

Last month we talked about Indirect Costs. These are usually thought of as costs required to support the field work, but not related to any one specific job. Examples include the cost of a shop, Project Managers, cell phones in the field for Supers or PM's, a truck that makes deliveries and pickups all day, and similar.

Many construction companies capture these costs in an Indirect Cost group on their financials, or at least under a job called 'Shop.' This allows the company to track costs in support of the field work, and later, allocate those costs across all the active jobs in the same time period.

So what are the options to determine how to allocate these indirect costs across all the active jobs? There are three that are common; **total number of labor hours**; **total revenue billed**; a **percent of total job costs.** We actually use two of these three in our own month end closing process.

Total Number of Labor Hours – To give an example, let's say you have $5,000 of indirect costs for the month. Let's also say that you have 100 hours of labor for the same time period across several jobs. Regardless of whether these are Regular/OT/DT hours, it's 100 hours of labor. So that's $50 per labor hour that will be charged to the active jobs. Job A has 58 hours, so that's $2,900 of Indirect costs; Job B has 8 hours, so that's $400 of Indirect costs; Job C has 32 hours, so that's $1,600; Job D has 2 hours, so $100. A Journal Entry is made debiting the Direct expense account and crediting a Contra account (there are other options) in the Indirect range with a job cost line item for each of the four (4) jobs.

Percent of Total Job Costs – In this method, we're looking at the costs for each job as a percent of the total costs. The costs would be higher if the work was overtime due to a holiday, winter conditions, or significant material purchases. In the scenario above, the $5,000 of indirect costs could be very differently distributed if Job 3 with only 2 hours also received a lot of materials that month; or if Job A had only labor, but the crew was heavily weighted with apprentices, for example.

Total Revenue Billed – This one is less common for our contractors. You may not be able to bill what you've earned due to restrictions or rejections from the GC or owner. So you may have months where the billing is too high or too low compared to the actual costs for the month. This works itself out in the over/under billing process (also called WIP), but is not the best parameter for Indirect cost allocations.

So how do you choose? We recommend running these scenarios for three different months, then looking at the end result. I'll bet this sounds like a lot of work, and it is! However, if you're an Excel wizard, that will be helpful; or you can use something like our Indirect Cost Allocation tool that integrates with Sage 100 Contractor. With our tool, you can choose the posting period (month) and run each of these scenarios, then compare the results.

Either way, adding the Indirect Costs to the Contract Work can be an eye-opener for your Estimators and Owners. The jobs have to make enough profit to support these indirect expenses. They're an integral cost to get the work done and they need to be considered when bidding the job. Once you have that worked out, you'll need to make sure there's enough left over to cover your overhead, and maybe something for that yearend bonus, too. – *CMW*

Collecting Time From the Field Just Got Exciting!

Want to love Monday's again? Check out our FIT System; new modules, new pricing. Join us **Thursday, December 19th, 1:00pm Central Time** to hear all about it!