Cyber Times
Newsletter by Secure ERP, Inc.
Insider Tips to Make Your Business Run Faster, Easier, and More Profitably

What's New

Even though it's summer there is no rest for the wicked or the education. This summer I hosted a presentation on cyber security with a discussion panel for a legal association. I also presented on privacy & cybersecurity for a major law firm's staff. Both were hugely received.

If you have an association or group, I'm ready to give them a presentation they won't forget. We'll ensure the attendees also get a weekly cybersecurity tip for the next year. No cost or obligation. Just contact our office to schedule. —Rick

August 2019

This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc. Secure ERP is a network security & ERP integration specialist in central Indiana with over 25 years of experience supporting small to medium sized businesses. Founded by a CPA and Cybersecurity Evangelist, Secure ERP is dedicated to protecting our clients' data and supporting their people and growth.

4 BIG Mistakes You're Making By Being Cheap With Technology

Technology is more affordable and accessible than it's ever been. Whatever you need is only a few clicks away, whether it's a product or a service.

But there are still many small businesses that cheap out on their technology and IT solutions. They just don't want to commit to quality hardware, software, security or backups – the list goes on. They go for the cheapest solutions, which often means they spend nothing at all. They don't commit to reliable security or current software. They're setting themselves, and their customers, up for disaster.

The question is, are you setting your own business up for disaster? Here are four HUGE mistakes you should do everything to avoid.

MISTAKE #1: You aren't backing up data. As convenient as it is to have all of your business's information in one place, such as a single local server or even a desktop PC, you're toast if anything happens to that hardware. For one, if you're lacking in IT security, you're making a cybercriminal's job easier. And two, if that hardware fails (as hardware eventually does; there's no way around this), you're left scrambling to recover that data and hoping it's still accessible.

You should never risk your business like this, considering how easy it is to back up your business's data. You can back up data on-site, get a cloud-based service or you can do both. The point is, you need to back up everything so you're ready should anything go wrong.

Once you have a solution, you can customize how your data is backed up. Do you need to back up data every day? Once a week? Once a month? It's up to you. Here's another thing to remember: your backup system isn't "set it and forget it." You need to check on it regularly and keep it updated to ensure your data is safe and ready to go should you need it.

Continued on pg.2

Continued from pg.1

MISTAKE #2: You aren't keeping up with the times. Speaking of keeping things updated, you should always update your software. Developers are constantly fixing bugs, patching software and improving usability. Skipping updates can leave you vulnerable.

Earlier this year, Cisco's Series 1001-X router was found to have a fatal flaw that opened it up to hackers. This flaw potentially gave hackers network access – and access to connected devices. This isn't the first router to have this kind of flaw and it won't be the last. Cisco pushed out an update to fix the flaw, but the update is useless if you don't install it.

Updates don't just apply to software; they apply to hardware as well. When you're running old hardware, that hardware is more likely to fail. It's already been put through its paces. Over time, hardware performance degrades. Plus, the older your hardware is, the less compatible it is with current software. You don't have to invest in new hardware every year or two, but keeping up with the times keeps you on top of your game.

MISTAKE #3: You don't train your team. While most businesses hire people who understand certain software products, you can't assume they know everything about that software. Your business might use a certain CRM application in a very specific way. Proper training on your systems ensures everyone is on the same page – and that they are using the software to its (and their) greatest potential.

More than software training, your team also needs to be trained up on IT security. They need to know the risks and how to keep your business's data secure. Never assume your team knows about the latest threats to small business – or that they even understand the basics of safe web browsing.

While you need to have IT security in place and protecting your network, servers, PCs and so on, you need to make sure your team understands that security and the threats that are out there. Your team should also be aware of the consequences if any data becomes compromised.

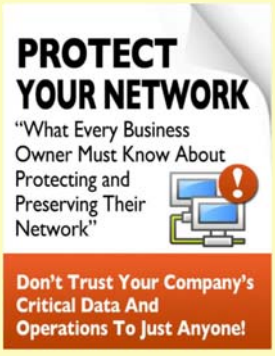
MISTAKE #4: You skip data security. Data breaches happen every day, and most of them go unreported. You only hear about the biggest breaches on TV or online. While major companies like Target or Facebook can more easily recover from a data breach (as they have a lot of money to throw at the problem), most small businesses can't.

If you're lacking in IT security, you're putting sensitive data at risk. This is proprietary business data as well as the personal and financial records of your customers. It can mean the end of your business if credit card numbers, names, addresses or phone numbers fall into the wrong hands.

Customers will no longer trust you. Your own employees likely won't trust you either, especially if their personal data is on the line, not to mention their reputation. When you skimp on IT security, you're about one step away from handing hackers and cybercriminals all the data you should be keeping under digital lock and key. When you invest in a solid IT security and work with experts who understand today's security landscape, these are things you don't have to worry about.

The bottom line is, if you don't invest in your business's technology and IT solutions today, you will pay for it tomorrow. You'll be dealing with upset customers if you get hacked, and you may end up closing your doors, temporarily or perhaps even permanently, as you attempt to recover lost data. Don't make these mistakes because you wanted to save money.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems



This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.secureerpinc.com/protect
or call our office at (317) 290-8702.

Cyber Security TIPs

HOW you're backing up is just as important as **WHAT** you're backing up in the era of hackers & ransomware.

Your data is precious and criminals KNOW it. This is why city gov leaders are paying over $600K (yes, that's six hundred thousand) in ransom for their data. One reason is the criminals target and destroy the backup which puts you with only one remaining option, pay up. The 2nd reason is triggered by HOW you backup. If you need to do a full restore of everything, that takes time and how you backed up will determine how long this recovery time will be. Recently a business owner had to do a full restore after a successful ransomware attack. Not only was the last good backup 5 days in arrears, but the restore took an additional 3 days. When it was all over, **the business lost 8 full working days.** That's 8 days of not being able to tell a customer what they owe or record ANY transactions.

Backing up to external hard drives, backing up data only, or tape backups no longer qualify for a proper business backup. We can explain why RECOVERY time & protection from ransomware is now the key. Ask us about it. —R²

Leading Like A Business Coach

When I meet with a team for a coaching session, I often find that everyone looks to me for all the answers. While I am there to help them get their priorities together and align their business and company culture, I'm NOT there to hold their hand through every decision that needs to be made. That's where the team leaders come in.

I look at my job as the "teach a man to fish" principle: I teach them how to think like I do so they can continue to have insightful and productive conversations when I'm not there. I want the leaders in my member companies to leave coaching sessions feeling comfortable about pushing their employees to be better, like I push them in the session. That is the ultimate measure of success for any business coach.

Here are a few key characteristics of a business coach that all leaders can and should adopt.

LISTENING
Hearing is the physical act of sound going into your ears, but listening is comprehending those sounds. The only way I can help people and groups improve is by knowing what works well and what their pain points are. They may not always say things you want to hear, but it's important that you not only hear them but truly listen. Don't immediately start problem-solving your way out of the conversation or you'll miss what's truly important.

LOOKING FOR WEAKNESSES
As leaders, we sometimes want to ignore weaknesses and problems because, frankly, it can be tough to admit they exist. You may hold some or all responsibility for them. But that's how a leader can push his or her company forward – by taking a high-level view and objectively finding the areas that need to be improved.

FINDING SOLUTIONS
After pinpointing shortcomings, figure out how to repair and strengthen them. It's not enough to acknowledge them; you also need to find solutions. Push your company or leadership team to sit down and brainstorm together. It's the best way to get everyone talking and to get others' perspectives on what will best address each issue. These sessions should be a regular part of the business's proceedings, not just when I'm there coaching.

LEARNING CONTINUOUSLY
It's helpful to know what leaders are doing in other companies. Read books and articles to see how others have improved their companies. Their solutions may work for you too, or they may spawn a brand-new idea you can implement. Even business coaches don't have all the answers, so take advantage of the world of resources at your fingertips to find a way around any roadblocks.

Leaders should never stop pushing and growing. That mentality will transfer to your team – after all, they are the ones who help keep your business going. Think, "What would Andy do?" and apply these principles in all meetings and company get-togethers, not just quarterly planning meetings. That's how the student can become the master.`

As the founder of Petra Coach, Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success, and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.

3 Things About Cyberspace You Should CONSTANTLY Remind Your Kids About

All parents need to closely monitor their kids' social media profiles as well as their use of tablets, phones and devices. It's no secret that sexual predators lurk online, looking for their next victim. While what you tell your kids should be age-appropriate, here's a list of things you ought to KEEP reminding them.

1. Everything you do online is public. If you wouldn't do or say it standing in the middle of your classroom with everyone present, don't do it online.

2. There is NO delete button. Removing comments and photos is like trying to take pee out of a pool.

3. Trust NO ONE online. Really bad, ugly, nasty people are online looking to fool you.

As for your older kids, you might remind them that schools and employers use social media to review you, so make sure what you post is what you'd want them to see.

The One Thing You Should Do Every Day To Be More Productive

At the start of your day, compose and send yourself an e-mail. This e-mail includes a list of tasks or goals you want to accomplish by the end of the day. As you get to work, review this e-mail then set the message to "snooze" until later in the day. In Gmail, snooze is the clock symbol on the right-hand side that appears when you hover over an e-mail.

Sending yourself a message is a great way to keep daily goals top of mind. Plus, writing down your daily tasks and goals helps you prioritize what needs to be done. When you tackle prioritized tasks, you work more efficiently. Then, when you have the e-mail in front of you at the end of the day, you can review what you've accomplished (or what still needs work), and you can celebrate the growth you made that day. Inc.com, 5/21/2019

Top Tips To Protect Your Remote Employees From Cyberthreats

Don't Use Unsecured Public WiFi

Unsecured public WiFi is everywhere: at cafés, airports, hotels and more. But these networks lack security, and it's easy for a hacker to snoop on your data. Hackers can even spoof unsecured WiFi networks and walk away with all the data they want with no one the wiser. Avoid them. Stick to secure networks you can verify as trustworthy.

Don't Keep Your Cyber Security "Best Practices" To Yourself

You may have your best practices, but do your remote employees know? Keep EVERYONE on your team educated and on the same page. When you have training, bring in your remote employees, or conference them in, so they get the same training. Send out regular updates about the latest cyber security threats and scams.

Don't Forget About Endpoint Security

Make sure your remote employees are utilizing IT security solutions on their ends, such as antivirus software, malware scanners, network firewalls and even a VPN for when they need to access unfamiliar networks. They should also be keeping their software updated with the latest available patches. Inc.com, 2/12/2019