Cyber Times

Newsletter by Secure ERP, Inc.

What's New

December Lunch & Learn

IN CPA SOCIETY

December 4th I'll be presenting on Cyber Threats & Solutions for the Indiana CPA Society.

Although this provides CPE for CPAs, we would love to have law firm partners, medical practice managers and business owners attend to learn how best to defend against hackers & ransomware.
Space is limited.
REGISTER HERE:
https://www.incpas.org/home/cpe-and-events/eventdetail?evt_key=0107e47e-3856-40cf-b452-e3e7df6f2a2f&SSO=true

November 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.

Don't Let Your IT Company Make This One Mistake With Your Computer Network

Your IT services company is one quick phone call away. This is true of a lot of businesses that outsource their IT needs through an IT services provider.

While having an outsourced IT company on standby is great, a lot of the time they *stay* on standby. That is to say, they only get a phone call when something goes absolutely wrong – networks crash, hardware fails, data is stolen or erased and so on.

This is a major mistake.

Your IT company is capable (and willing) to do so much more than react to a catastrophic failure. When you save the phone call for emergencies, you're leaving a lot of expertise on the table. Your IT company can make a huge difference in the way your business operates day-to-day – and for the better!

CONSIDER THE FOLLOWING:

You reduce your risk greatly. Do you know if your systems and processes are compliant with current standards? Is your network security up to par? Do you want to risk it and assume everything is up to snuff? Your IT company is there to make sure your business is secure before something happens, whether it's a minor network outage or a catastrophic security breach. If you're storing your customers' financial details (or, really, any sensitive data) on a local server, this is HUGE.

You have one less thing to worry about. When you delegate and rely on your IT services company, this frees you up to work on what really matters: your business itself. Your IT company helps make sure you don't spread yourself too thin. And when it comes to delegation, make sure your employees can contact your IT team as needed. After all, your employees are on the frontlines and may experience an issue that needs resolving. They shouldn't need to bug you about it. They should be able to submit a ticket directly to your IT. Simple!

Your business stays ahead of the curve. This comes down to proactivity. An experienced IT company knows IT like no one else; they can, in some cases, catch a problem *before* it becomes a problem. They are there to keep your network updated and maintained, and, should an issue arise, they can address it ASAP to ensure your business avoids any downtime or outages. Plus, this gives you a competitive advantage. A lot of medium and small businesses skimp on security. They spend as little as possible on security and network management. You know who doesn't skimp? The bigger companies. You can get on their level and blow past your competition.

> **"Waiting until something goes wrong is a dangerous and ineffective approach to IT. It puts your business at serious risk ... "**
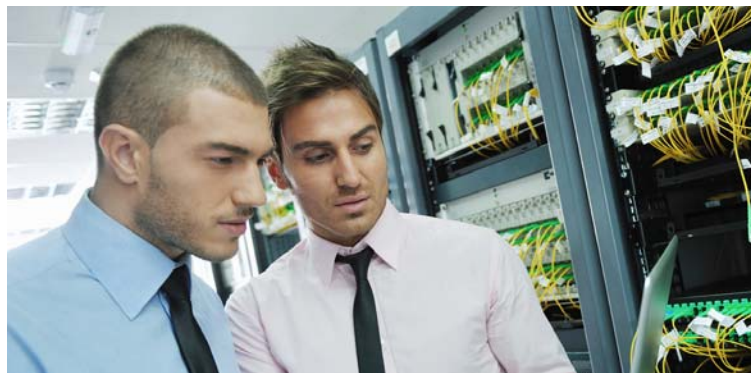
This is something your own customers would love to hear.

You keep costs down. Business owners love to save money where they can. Outsourcing your IT *and* relying on your IT company helps you do this. First, you don't have to hire a dedicated, in-house IT team. This can be *very* costly. A qualified IT staff can come with a serious price tag because they're in such demand. Second, because you have an outside IT company maintaining your network, they can help you avoid costly disasters, such as a network failure or data loss.

Waiting until something goes wrong is a dangerous and ineffective approach to IT. It puts your business at serious risk, both internally and externally. Let your IT company do what they do best: managing your systems! They help keep things running smoothly. You never have to worry if your firewall is up and running (and up-to-date). Don't keep them at arm's length. Let them do their job.

Cyber Security TIPs

There's a proverb which asks "When is the best time to plant an oak tree?" "20 years ago." is the answer. "When is the 2nd best time?" "Tomorrow." The moral of the story is to start as soon as you can.

Start planning for a security threat NOW.

Decisions and judgments made during this time are driven by emotion and not facts. Things to consider when you're planning:

- 3rd Party members to be vetted by your Insurance Co.
- Physical access
- Lost or stolen mobile devices
- PCI (payment card industry) or HIPAA compliance
- Security incident response
- Threat monitoring
- Dark Web monitoring
- Identity Theft Protection
- An attorney experienced with breach response is critical
- Reputation & PR Mgmt

Don't have an IT pro on staff? We'll act as your virtual Chief Information Security Officer (CISO) for your technology security. A Security Awareness Solution is a great start: http://bit.ly/seitraining2

There are great resources out there for businesses that just don't know where to start with cybersecurity. Take a look at https://www.fcc.gov/cyberplanner for a customizable guide to where to get started with operational and organizational planning. - R^2

5 Secrets To Increasing Your Prices

We all have to raise prices at some point in order to stay solvent. Many people agonize over the decision, worrying about what the net effect on their business will be. Here are some tried-and-true strategies I've learned that will make your prudent business decision even more effective.

1. CREATE A NEW LABEL.

Language is powerful, and if you're using the standard, generic industry label for your product, then you're going to have a harder time charging a premium price. When I owned my computer forensics business, "data imaging" was the term the industry used for retrieving and storing information from a computer. I wanted to differentiate my services from the rest of the pack, so I added some bells and whistles that the other guys didn't, and I called my service "data encapsulation." When you use a new term, you can get a client to ask, "What does that mean?" That's a chance to differentiate yourself from the crowd and justify your premium price.

2. DON'T CHARGE BY THE HOUR.

Think about it: if you charge by the hour, then the better and more efficient you become in your field, the less money you make. Charging by the project rewards efficiency because as your skills and speed improve, you'll be able to complete more projects, which increases revenue.

3. INCORPORATE PACKAGING/BUNDLING.

I once worked with a client who was looking for a way to improve his profitability. His problem was that he sold iPhones on eBay, and thousands of people were doing the same thing, which drove prices down. Our solution? He created a DVD that shared insider secrets for the iPhone and bundled it with iPhone purchases. He combined products, creating a unique package that no one else could offer, which allowed him to raise his prices.

4. JUST DO IT.

Your best customers will be surprised that you didn't raise prices sooner because they value your work. It's possible that you'll lose a customer or two over your increase, but those clients who leave are likely to be your problem children anyway. If you're not confident about how your customers will react, introduce a price increase for new customers only and see how it goes.

5. EXPLAIN.

In the absence of an explanation for your price increase, your customers will invent their own. They may speculate that you're greedy and taking advantage of them. If you take time to explain why you've increased prices, though, you'll find that your customers will accept the change much more easily. Cite your increased expenses, your expanded staff and your commitment to improve quality, and your clients will support your decision.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal; *MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book* The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan, *has already been called "the next E-Myth!" For more information, visit mikemichalowicz.com.*

■ The Biggest Cyber Security Risk Your Business Faces

Remote employees pose a huge risk to businesses. When they connect to the Internet, whether out and about or at home, you have no idea how secure their connection is.

Plus, a majority of small businesses don't regularly update their remote work security policy, and upward of 30% of small businesses don't even offer any kind of security training. If your remote employees are accessing sensitive data, the risk for your company is huge.

Nearly 60% of small businesses hit by a cyber-attack go out of business within six months of the attack. They simply cannot respond and recover. It's expensive, and customers often flee.

One way to avoid this is to have a cyber security policy in place. Your employees should be following your remote work rules. On top of this, a cyber security insurance policy can help you avoid the cost of recovering should the worst happen. *Small Business Trends, 8/19/2019*

■ 4 Everyday Habits Smart People Use That Destroy Productivity

1) They need to be connected. The news and social media are always updating – it's addicting and people are afraid to miss out. They may also be distracted by text or e-mail. Cut yourself off to find focus.

2) They multitask. Some people say they are great multitaskers, but research says it just doesn't work – not if you want to focus and deliver quality results. Multitasking splits focus and harms productivity. Do one thing exceptionally well before moving to the next task.

3) They don't write things down. Don't over-rely on your memory to get things done. We can get overwhelmed throughout the day and forget things. Write things down, take notes or make lists to avoid this common mistake.

4) They focus on wants. Sometimes our "wants" get in the way of our "needs." You can't be productive if you're too focused on wants. Buckle down and focus on what needs to get done. It comes down to self-discipline.
Business Insider, 7/12/2019

■ 3 Easy Ways To Cut Down On Mobile Data Usage

1) Monitor and customize your usage. Most current smartphones let you see how you're using your data and what you can do to change your habits (turning off apps to save data, for instance). You can also turn off data anytime you don't have use for it.

2) Use WiFi Assist or Adaptive WiFi. You can set your phone to automatically connect to trusted WiFi hot spots when in range. This is a great tool if you often forget to switch manually.

3) Download content when on WiFi. When you know you're going to want to watch a video, TV show or movie when you're away from WiFi, many apps let you download content to your phone. *Mashable, 8/20/2019*

© MARK ANDERSON, WWW.ANDERTOONS.COM

"I'm *trying* to back it up, but I can't find reverse."

ANDERSON