Cyber Times

Newsletter by Secure ERP, Inc.

Insider Tips to Make Your Business Run Faster, Easier, and More Profitably

FREE Executive Seminar Breakfast:

"CYBER SECURITY AND THE WAR TO STEAL YOUR ASSETS: WHAT YOUR BUSINESS NEEDS TO STAY SAFE AND STAY OPEN FOR BUSINESS"

Owners, C-level executives, and managers should attend to learn what critical protection every business must have in place NOW to avoid cyber-attacks, a data breach, compliance penalties, and the latest cyber threats, like ransomware.

When: Thursday, September 14, 2017, 8–10 a.m.

Further details and reserve your spot by registering at www.secureerpinc.com/seminar

August 2017

This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc.

Secure ERP is a network security and ERP integration specialist in central Indiana with over 25 years of experience supporting small- to medium-sized businesses. Founded by a CPA and Sophos certified security engineer/architect, Secure ERP is dedicated to our clients' security and growth objectives.

The ONE Thing You Must Do to Keep Your Data Safe in the Cloud

Is Your IT Guy Doing This?

How secure is *your* data? Cloud data storage is becoming a massive industry in this country, and many businesses and other institutions are putting their data into the cloud. Some of this data is pretty harmless. Other stuff — like hospital records, banking information, or company payrolls — are prime targets for bad actors. Is the cloud storage tradeoff worth it?

The short answer is yes, but only if your IT guy is encrypting your sensitive data.

Every cloud storage company you talk to will claim to take top-of-the-line security measures on behalf of your data. But that, in a nutshell, highlights the problem with cloud storage. Your data is entrusted to a third party for safekeeping. It's possible that they'd do everything in their power to safeguard your information. But bad things, like ransomware, phishing, or just plain going out of business, *do* happen. And when they happen, it's not the cloud storage company whose data is on the line; it's *yours*.

Even if that doesn't occur, let's be honest. Most of the major cloud storage companies are based in the United States, the U.K., or France, where they could be subject to NSA snooping (or questionably legal surveillance from any other government entity). Despite the best efforts of many storage companies to prevent government intrusion, your data could still be at risk, even when it's locked up tight.

This brings us back to encryption, which is the hands-down best way to protect your data, period. It's just like locking sensitive data in a box, with a password needed to

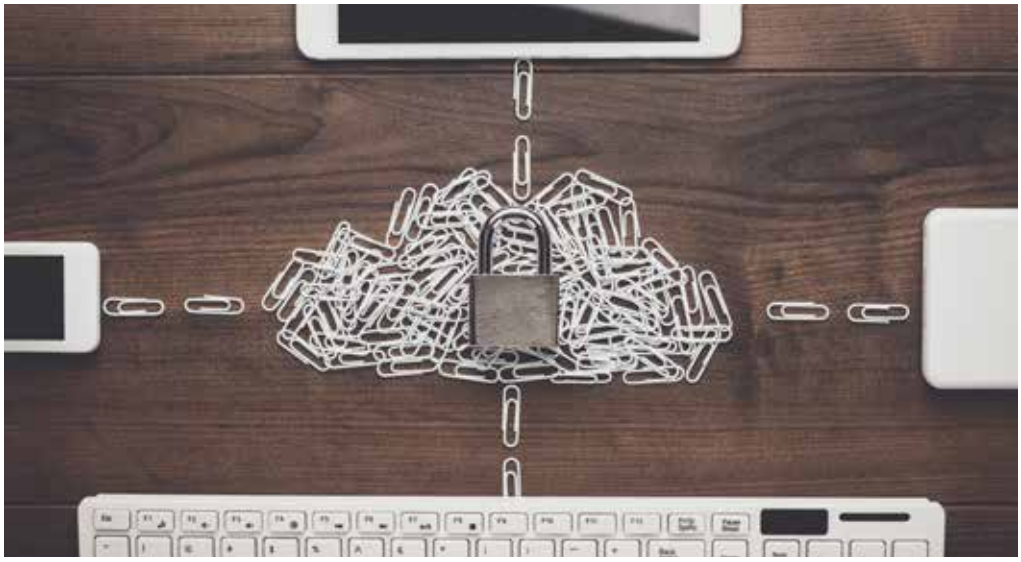
continued on pg 2 ...

continued from cover ...

reopen it. Even if someone gets ahold of the box, if they don't have the password, there's nothing they can do with it. You can encrypt data yourself with free tools. There are a lot of encryption tools out there, and you'll want to make sure that you have the right one for your specific needs. If you ever need a recommendation, don't hesitate to reach out and ask! We'll be happy to provide you with the specific recommendation (free or paid) that fits your needs.

In addition, most cloud storage companies protect your data with their own encryption, but this isn't as secure as encrypting your own information. That's because the cloud storage company has the encrypted data in its possession, but it also has the *keys* to that data. If someone can get in, they can probably get the information they want. And a disgruntled employee — or just a hapless one — can also provide hackers access to the system through good old-fashioned human engineering.

If the cloud storage company is compromised (and it happens quite often), will your data be secured or unsecured? Well, if you're encrypting your own data before uploading it, then the bad actors will open up the safe to find … a bunch of locked boxes. Pretty frustrating, right?



On the other hand, if you've trusted the cloud storage company to take care of everything, you're going to have a bad day.

As you can tell, it makes sense to have your IT guy encrypt everything that gets put on the cloud *before* it gets there. But remember, just as your cloud storage provider is vulnerable, you can be vulnerable as well. It's less likely that bad actors will target your company specifically, but if they want your data bad enough, they'll go to great lengths to get it.

Many people have a misconception that these criminals will just use a magic program to crack your encrypted files. Decryption *does* exist, but it requires a lot of time and processing power. It's far more likely that hackers will target your email or other aspects of your system and try to find out the encryption codes that way. And never forget that people are the weakest part of your IT security. Educate employees so they aren't vulnerable to phishing scams, downloading questionable software, and visiting the wrong websites.

Present a "hard target" when it comes to your cloud storage, and seriously, encrypt your data before you put it online. If your IT guy isn't doing that already, you need a new one.

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

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

Download your FREE copy today at www.secureerpinc.com/protect

Cartoon of the Month

continued from page 4 ...

"pull the wool" in person, so use Craigslist and follow their safety guidelines for great deals. *gizmodo.com May 11, 2017*

Can a Surgeon Really Use an App to Practice Surgery?

Touch Surgery is an app that lets anybody "operate" in dozens of realistic surgery simulations. Around the world, there are plenty of places with just one or two doctors within driving distance, and those physicians have to undertake procedures they may not be trained for. A few hours with Touch Surgery on the smartphone — or, for added realism, the Hololens — can mean the difference between a bad outcome and a good recovery for the patient. *digitaltrends.com April 14, 2017*

FBI WARNING

In May the FBI issued an alert on a **FIVE BILLION DOLLAR** scam occurring right now. Even one of our clients was contacted and through education & training recognized it as a scam before sending the criminal money and costing the company over $5,000. We're currently working with the FBI on this event. Here's the alert: https://www.ic3.gov/media/2017/170504.aspx

We can help you implement the three best strategies to defeat these criminal scams:

- Employee education and training
- Implement strategic financial communication
- Implement technology to prevent faked emails from impersonating company executives.

ACTION NEEDED: Send me an email at rrusch@secureerpinc.com or call (317) 290-8702 to schedule a **FREE test** of your company's email to see if YOU can be impersonated.

Geoff Smart: 3 Ways to Get Your Life Back

I was once meeting with an executive, and I noticed a small framed sign on her desk that read, *Eat Lunch.* When I asked about it, she said, "My job is all-consuming. If I am ever able to eat lunch, I'll know that I got my life back." Sound familiar? So many of us are capable business leaders and yet powerless to reclaim our lives from our jobs. But work is not supposed to be like that. And, if yours is, you need to do all three of the things I've listed below. Sorry, but to really get your life back, you have to do them all.

First, set personal goals, like how many nights per week you want to eat dinner with your family. Setting and tracking goals works. A CEO of a $20 billion company set a goal to be home from 6–8 p.m. (to spend time with his teenager) at least four nights a week, and he often beat that goal. An extremely busy tech entrepreneur set a goal to have a proper cellphones-off, two-week vacation every summer. An executive assistant in our New York office always wanted to coach her daughter's soccer team, so she finally set the goal and did it.

Second, schedule personal time. I recently called a colleague at midday on a Thursday. He was at the zoo with his wife and two kids. We have a "freedom and flexibility" culture at ghSMART. If somebody is trying to schedule your time over one of your personal commitments, tell them you are not available. It's none of their business why you are not available. It's not either-or. You can be successful and have a life.

Third, delete, delegate, delay, and then (as a last resort) do. I saved the best tactic for last. Is your first instinct to do whatever the urgent, flashing, text-chiming, inbox pop-up task demands? That's a lousy way to work, and it's no way to live your life. Follow this sequence instead:

- Your first instinct should be to **delete** any task. Sorry, task! You don't own me.
- If it has to get done, **delegate** it to a capable person who can do it.
- If there is nobody to delegate it to, then **delay** the task until a time that works for you.
- If that is not practical, then your last resort is to **do** that task now.

If you set personal goals, schedule personal time, and practice the delete-delegate-delay-do framework, you will find you can achieve career success and get your life back. And if you think these tactics are useful, please download our other free leadership tools at geoffsmart.com/smarttools

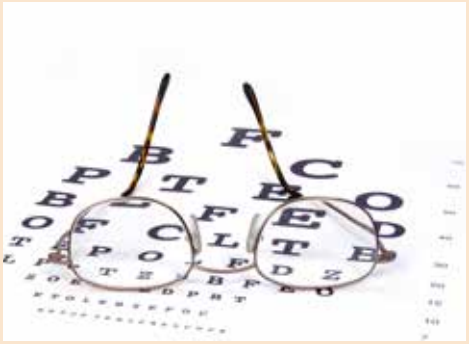
Dr. Geoff Smart is the No. 1 thought leader for the No. 1 topic in business: hiring and leading talented teams. Dr. Smart founded the leadership consulting firm ghSmart in 1995, a firm he still chairs today. He is also a nonprofit founder, government advisor, and Wall Street Journal best-selling author.

6739 Cobden Lane
Indianapolis, IN 46254

Inside This Issue

The Shocking Secret About Bank Fraud That Practically No Small Business Owner Knows, But Should

Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is NOT responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding money stolen from your account!) Many people think FDIC protects you from fraud, but it doesn't. It protects you from bank insolvency, NOT fraud. Here's a quick tip: Set up email alerts on your account so you are notified any time money is withdrawn. The FASTER you catch fraudulent activity, the better your chances are of keeping your money. If you contact the bank IMMEDIATELY, you have a very high probability of foiling a hacker's attack. *Oct. 28, 2016*



How to Get an Eye Exam WITHOUT Leaving the Comfort of Home

Glasses company Warby Parker is making the jump from mail order to medical diagnoses with their new Prescription Check app, which lets you test your eyes at home. Of course, some restrictions apply — like being a Warby Parker customer, living in a handful of participating states, having no history of eye disease, having received a real eye exam in the last five years … you get the idea. Still, it's a very cool idea and perhaps a herald of things to come in the world of remote medicine. *engadget.com May 23, 2017*

How to Buy a Secondhand Smartphone WITHOUT Getting Ripped Off

There are great deals to be had on used electronics, but there are also pitfalls. Our advice? Start by being realistic, do plenty of research on real-world prices and conditions using sites like eBay, and buy immediately after the holiday season or when a new version of what you want comes out. As for those pesky scams, it's much harder to

continued on pg 3 ...