

Cyber Times

Newsletter by Secure ERP, Inc.

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

FREE Cybersecurity Seminar

COMING THIS SEPTEMBER

We are in the planning stages of offering an informative (not salesy) agenda on Cyber Crimes & Criminals and how you can keep your business safe. We'll cover the following:

- Current Threats & What's My Risk
- Solid, Simple Steps Any Business Can Take Now to Be Safer – Some are even FREE
- Effective Risk Management – How it can save your company's bacon

Watch next month's newsletter for details or email me at rrusch@secureerpinc.com to reserve your spot now!

June 2017



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 & Sophos certified security engineer/architect, Secure ERP is dedicated to our client's security & growth objectives.



The Hidden Dangers Of 'Shadow IT' To Your Business

We all know that using information technology — programs, apps, or internet browsing — carries a certain amount of risk. Nobody wants to have their secure data compromised, but technology brings enough benefits that the risk is worth it. So you vet certain systems, you establish protocols, you update and patch your software, and you keep track of the technology used at work.

But what about the technology your employees are using that *isn't* part of your official plan? We're talking about messaging apps, Excel macros, cloud data storage, collaboration spaces, and even hardware like USB drives, smartphone storage, and personal laptops that you don't control.

We call this "shadow IT," and that's a whole lot of potential holes to cover!

Even if you ignore the dangers of having accounts hacked, data stolen, and websites vandalized, shadow IT can be very inefficient. You don't control it, so you don't know where important information is or what work is being done. It makes it hard to avoid duplication of efforts and even harder to manage employee productivity. What are you to do?

Well, your gut reflex might be to "crack down" on using unauthorized technology for work purposes. Swallow that reaction, though — you can't stop it, and you'll just harm morale. You'll also drive usage even further underground; your people won't be honest with you for fear of reprisal. That means that if a compromise occurs, you'll be the last to know.

Instead, keep an eye on the situation. Make it clear that you support employees using the tools they need to get the job

continued on pg 2 ...

continued from cover ...

done, as long as they let you know what those tools are. If your people start using cloud storage apps, that's fine — but have *them* explain how they'll keep that data secure. Just as you empower them to find their own tools, empower them to keep things secure.

You probably can't come up with a list of all the shadow IT that's being used at your work, but you can keep an eye on the trends as they develop. Research the technology that's being used and watch the headlines for data breaches or other compromises.

“Don't try to stop all shadow IT use; you'll only guarantee that when a compromise occurs, you'll be the last to know.”

In some cases, you will have to crack down on specific apps, programs, or devices being used at your work; they're just too risky. If you've worked with employees and fostered good communication, this



shouldn't be an issue. Remember to avoid blaming employees when shadow IT becomes a problem — especially if they bring the issue to your attention themselves. There's nothing wrong with asking your people to stop using a specific program or device, as long as you're transparent and have good reasons.

Last, but not least, try to look on the bright side. Shadow IT may be a little risky, but it

also presents opportunities for employees to drive productivity and try out new best practices. If they're using a piece of technology, it's probably doing something that the currently "approved" tech is not. They're also showing self-starter tendencies and trying to do their job better. And that's always something you should support!

Free Report Download: The Business Owner's Guide to IT Support Services and Fees

You'll learn:

- The three most common ways IT companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees, and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration, and added costs later on that you didn't anticipate.

Claim Your FREE Copy Today at www.secureerpinc.com/itbuyersguide



Cartoon of the Month



continued from page 4 ...

who dominated the tablet market for years. Microsoft tablet functionality won out over Apple's iPad; the non-third-party keyboard probably helped with that. But Microsoft also won in the design category, which has to sting. Surprising nobody, LG, Asus, Samsung, and Acer came in far behind Apple and Microsoft. *Mashable.com April 7, 2017*

PANTHER DRONES strutted their stuff recently with capability to fly *and* roll along on land, delivering packages with aplomb. Similar to military-style land-and-air drones, the Panther has a few advantages when it comes to residential delivery — like avoiding air hazards such as trees and power lines. Unfortunately, the Panther is relatively heavy, so it has a limited range compared to other prospective delivery drones. *Discovery.com March 30, 2017*

Security Tip This Month

Your employee wants to work from home and was smart enough to ask you if they can use a “free” application (maybe DropBox) to share files back & forth. But how do you know the free app is safe for your business data? [Here's a cyber security tip:](#)

Ask the vendor for a **HIPAA Business Associate Agreement**, also known as a HIPAA BAA.

Being HIPAA compliant has strict regulations on data security. If they won't provide it, don't use it!

Oh, and here's a question to ask your 3rd party vendors who touch your computer systems like ERP solution consultants & IT Service providers. In other words, guys like us. Ask them for their Certificate of Insurance regarding Errors & Omissions. If they make a negligent, costly mistake with your data, you won't be stuck covering the tab.

Time to Get Vulnerable *By Darren Hardy*

When you hear the term “leader,” adjectives like strong, assertive, and powerful come to mind. But what about vulnerable? Those in leadership positions often believe that displaying vulnerability to their team is a sign of weakness.

I'm here to tell you that they couldn't be more mistaken. In reality, vulnerability is a strength, and all skilled leaders have it. And in order to help you grow into a better leader, **I want you to be vulnerable.**

Patrick Lencioni once said to me, “Start by coming to terms with your own vulnerability as a leader and then translate that to your team and then the rest of the organization.” Waldo Waldmen, a top fighter pilot and a good friend of mine, once said something similar. He explained that after every mission, they would have a debriefing. Before it started, everyone was required to *take off* their name tags and their rank. Now, with an even playing field, they would go over the good, the bad, and the ugly of the mission. The leader would take the lead, admitting their own mistakes first.

They call this “exposing your chest to daggers,” and it creates an environment for the new hires, the young wingmen, and the young folks that are in the formation to say, “You know what? If so and so, the flight lead, or so and so, the top gun, is going to share his or her mistakes, then I can do the same thing.” But it has to come from the top down, and it means being vulnerable, more honest, and more open about what's going on. Waldo said the key is to show you are a human being first and a top gun or high-ranking officer second.

Do *you* start meetings by exposing *your* mistakes first?



Darren Hardy is the creator and visionary behind SUCCESS magazine as well as the New York Times best-selling book “The Compound Effect.” His newest book is “The Entrepreneur Roller Coaster.” For more, visit darrenhardy.com.

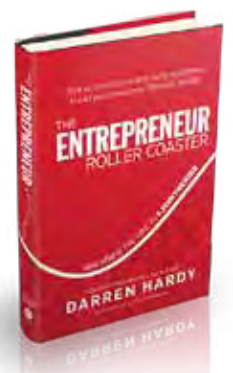
I'm not talking about being passive-aggressive. “I never should have trusted so and so with this.” I see and hear that all the time, and it's the opposite of exposing your chest to daggers. I'm talking about where *you* underperformed, did something wrong, or made a bad call. Those are the things to expose.

Many years ago, Les Brown gave me some great advice. He said, “You are a compelling speaker and certainly you have had a tremendous track record of success — but you can't just talk to people's heads or only appeal to their intelligence.” He continued, saying, “They have to feel your story, the whole story — failures, shortcomings, fears, and pitfalls — both the triumphant and the terrible.” That, he told me, was what would make me a real leader.

As you can imagine, this was an awakening, and it changed my life. You'll notice it if you read my first book and my new one; “The Entrepreneur Roller Coaster” is a lot more honest about my personal journey, warts and all. While people may be inspired by your success, they are *empowered* by knowing that they can fail at times and still succeed wildly.

If you want to be a leader, open yourself up to others. If people can feel and connect with you, they will charge through walls for you. That is real leadership, real influence, and real achievement. So, right now, think of one failure with which you can open up to your team.

Are you in? I promise you will see immediate results.





PRST STD
US POSTAGE
PAID
BOISE, ID
PERMIT 411

6739 Cobden Lane
Indianapolis, IN 46254

Inside This Issue

Hidden Dangers of Shadow IT to Your Business | 1

Free Download: What Every Business Owner Should Know About IT Support Services and Fees | 2

Why This Leadership Quality Is a Sign of Strength, Not Weakness | 3

TWITTER might be building a paid subscription service for “power” users. According to *The Verge*, the social media giant is surveying users to determine the size of a market for pay-to-play tweeting. This would mean a more robust platform of tools for marketers, journalists, and others who want the most from Twitter. This comes at a rough time for Twitter, and any potential influx of revenue has to be a welcome thought. *TheVerge.com*

THE CHARGING TOWER is a new concept that *Digital Trends* recently reported on. The idea is to replace current gas stations with charging stations in the future as electric cars become more popular. Stacking up cars like dominoes, the tower looks more like a parking tower than a gas station. This is important because electric car technology seems to indicate that charging will take hours longer than a standard “gas-up” takes today. *DigitalTrends – April 6, 2017*

MICROSOFT won the J.D. Power tablet survey, as reported by *Mashable*.



Although the “tablet wars” of the past aren’t as hot as they used to be, it’s still an upset (albeit a close one) for Apple,

continued on pg 3 ...