Cyber Times
Newsletter by Secure ERP, Inc.

What's New

Starting off an exciting year, Secure ERP sponsored a table at the Indiana Manufacturers Association 2017 Legislative Briefing and Reception. We met with several manufacturers to discuss SYSPRO ERP software. On February 14th we're excited marks our first event as a business partner of the Indiana Chapter of the Association of Legal Administrators. We know some networks need some extra love right now. . If you've dealt with viruses & costly downtime, we'd love to take away the "hurt" so it never happens again.

February 2017

This Publication is provided courtesy of Rick Rusch 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.

Cloud Computing: Good, Bad & Ugly

When a network of IoT gadgets like routers, DVR machines and closed- circuit TVs can take down hardened, well-provisioned Internet giants like Twitter, Spotify and Amazon – as happened last October – you've got to think twice before moving your data to the cloud.

Yes, a move to the cloud can yield big payoffs in terms of cost savings, increased efficiency, greater flexibility, collaboration for your workforce and more. Yet there is a dark side. It would be naive to think otherwise. Your choices about whether and how to use cloud technology in your network merits serious consideration.

So, just what is "the cloud"?
Instead of constantly buying new equipment and software, cloud computing allows you to pay for just what you need. Just as with a utility company, you get software and storage on a monthly basis, with no long-term contracts. Chances are, most of the software you now use is cloud-based. You simply access it on a pay-as-you-go basis.

Similarly, you can store data in the cloud, where it can be easily accessed when you need it. This reduces the need to buy and manage your own backup gear and software, thus reducing overhead. Yet, as with any major decision, it's critical to be aware of both the benefits and pitfalls of putting your company's data in the cloud.

The Pros
There are three major advantages offered by cloud computing:

1. **Flexibility**. Scaling up or down can be done without major investment or leaving excess capacity idle. It also enables your entire workforce to get more done, where and when they need to.

2. **Collaboration**. With data and software in a shared cloud environment, staff can collaborate from anywhere. Everything from HR to accounting, and from operations to sales and

continued pg.2

customer relations, can be managed from diverse and mobile environments, giving your team greater power to collaborate effectively.

3. Disaster Recovery. Typically, data stored in the cloud can be easily retrieved in the event of a disaster. It also augments local backup and recovery systems, adding protective redundancy.

The Cons

While the cloud offers obvious benefits, it also increases your company's potential "attack surface" for cybercriminals. By spreading your communications and access to data beyond a safe "firewall," your network is far more exposed to a whole bevy of security concerns. Many of them can be addressed with these three best practices:

"Keep verifiable anti-malware software in place throughout your network at all times."

1. Social Engineering Awareness. Whether you go cloud or local, the weakest link in your network is not in your equipment or software; it's in the people who use them. Cybercriminals are aware of this fact. And you can count on them to come up with an endless variety of ways to exploit it. One day it's a phone call ostensibly from your IT department requesting sensitive data, the next it's an email that looks official but contains malicious links. Make sure your employee are aware of and trained to deal with these vulnerabilities.

2.Password Security and Activity Monitoring. Maintaining login security is absolutely critical any time you're in a cloud environment. Train your staff in how to create secure passwords and implement two-factor authentication whenever possible. Take advantage of monitoring tools that can alert you to suspicious logins, unauthorized file transfers and other potentially damaging activity.

3. Anti-Malware/Antivirus Solutions. Malicious software allows criminals to obtain user data, security credentials and sensitive information without the knowledge of the user. Not only that, some purported anti-malware software on the market is actually malware in disguise. Keep verifiable anti-malware software in place throughout your network at all times, and train your employees in how to work with it.

Free Cloud Readiness Assessment Reveals Benefits And Pitfalls For Your Company From A Move To The Cloud

During the month of February, we're offering a FREE Cloud Readiness Assessment for any Indianapolis company with 10 or more computers and a network server. We'll come to your office and conduct a complete review of your computer network, data, software and hardware and how you work. We'll then give you helpful answers and insights about cloud computing for your business – all at no cost or obligation to you.

Claim your free Cloud Readiness Assessment today at www.secureerpinc.com/cloudreview or give us a call at 317-290-8702.

Free Report Download: The Business Owner's Guide To IT Support Services And Fees

You will learn:

- The 3 most common ways IT services 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, frus- tration and added costs later on that you didn't anticipate.

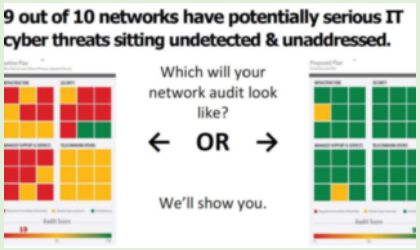
Claim Your FREE Copy Today at www.secureerpinc.com/ITbuyersguide

Vulnerability Testing vs. Penetration Testing (Pen Test) - Which Do I Need?

Businesses are being told they need to perform penetration tests to gauge the security of their network. Firstly, ensure you're actually buying a true pen test. True pen testing is performed by a human being, not automated, and extremely costly, as in 5-figures costly.

Secondly, prior to pen testing businesses should start with vulnerability audits. Costs are quite reasonable while identifying exactly what your IT professional should focus on to ensure your company's protection. Once the vulnerabilities are addressed, pen testing may be used to ramp up your cyber security protection to the next level.

Need to discuss it in detail? Give me a call to see what makes sense for your firm.



3 Ways Leaders Build Trust In Their Team

Warren Buffett once famously said, "It takes 20 years to build a reputation and five minutes to ruin it." While that may be true of public perceptions held by those outside of an organization, a leader's reputation within their company should be far more stable – as long as that person is working daily to build a reputation among team members as dependable and trustworthy, that is.

Trust is contagious. If team members are to become more honest and reliable, a leader needs to start by demonstrating those qualities. Building trust within an organization must be intentional. When leaders get it right, it boosts productivity, increases positivity and builds positive relationships throughout the company.

Here are three steps to building trust within an organization:

Do What You Say

This is the foundation. It may seem obvious, but not following words with actions is often the first mistake leaders make. Because there is not always someone holding the person in charge accountable, it can be easy for higher- ups to feel entitled to do something other than what has been promised. Let's face it – employees can be too intimidated to call out the boss (out loud to their face, anyway).

A leader should always be honest and reliable in their words and actions – even when it comes to things as simple as showing up to meetings and sticking to agendas. People are watching, and it matters to them. If team members feel they can't trust someone on the small stuff, there's no way they'll trust their supervisor with larger or more important things.

Ask About the Personal Things

It can be difficult to know whether someone deserves a celebration or needs help without making it a point to find out what's going on with team members. Setting up a recurring time to ask how things are going can encourage people to share.

Some may be reticent to voice personal information at work, but there are ways to open the conversation. Ask questions like "What were your personal highs and lows over the past week?" If a team member has difficulty opening up, lead by example. Sharing a personal story first demonstrates that you have sufficient trust in your team to share their personal lows. Then team members will be more likely to follow.

Learn Together

Nothing works to build trust in a team as much as learning together does. Find opportunities to travel to a seminar, go to trade shows or even hold recurring lunch-and-learn meetings with a different leader each week. The benefits of traveling and learning together are numerous, but the most important, positive outcome just might be the deep trust that can develop through those shared experiences.

Trust is essential in order to have a healthy organization – between executives, team members and among the entire staff, no matter how large or small. By being an active participant, and staying reliable and open, leaders help their teams work more efficiently and with greater passion for their work.

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. After all, as he tells his clients, 100% annual growth is only 2% growth every week. It's not easy. But possible. Andy learned how to build great organizations by building a great business, which he started in college then, grew into an Inc. 500 multi-million dollar national company that he successfully sold and exited. He founded Petra to pass on to other entrepreneurs, business own- ers and leaders the principles and prac-tices he used to build his successful enterprise, which are rooted in the Rockefeller Habits methodology.

Traditional home security firms desperately hope you won't try this system.

If you want to protect your home from break-ins, you can pay monthly fees of $45 or more and lock yourself into a long-term contract with a traditional home security firm. Or, for $230 you can get a five-piece Simplisafe Starter System, featuring an entry sensor, motion detector and keychain remote. It takes about 30 minutes to set up and triggers a 105db alarm in the event of a break-in. Upgrades include extra sensors, "panic button" for your bedroom and surveillance video camera. You can also add a cellular connection that notifies police if and when a break- in occurs, for just $14.99 per month – less than a third the cost of traditional systems.

-ASecureLife.com

This billion-dollar start-up is busting cybersecurity's biggest myth.

In 2011, hackers were slipping through cybersecurity company MacAfee's software at an alarming rate. Their CTO at the time, Stuart McClure, had to make a lot of apologies to their clients for the intrusions. In 2012 McClure left MacAfee to start a new company, Cylance, which focuses on prevention, not just detection. Contrary to common belief, all that most anti-malware programs can do is detect a breach once it occurs. Once detected, it can take six to nine weeks or more for a patch or update to be published. Cylance, on the other hand, now valued at $1.1 billion, uses AI and machine learning to detect and defend a network's weaknesses before hackers can exploit them.

-Inc.com

Ask these six questions before spending a dime on a promotional video for your company.

Do you want it to... 1) Attract more prospects via branded YouTube or other channel? 2) Act as a freemium to attract prospects, or a premium to incentivize them to buy? 3) Teach customers how to get the most out of your product or service? 4) Be part of a video blog (aka "vLog") and drive traffic to your website? 5) Welcome new customers to your business, show them how to access and/or use what they just bought and give them a chance to see your smiling face? 6) Or do you want people to pay you to view it, as with online training?

-Entrepreneur

"The arrow is free, but for a small fee I also offer an upgrade with flowers and candy."

These glasses open up a whole new way to share your world.

Snap Spectacles let you shoot video from your glasses. Which may not set off a tech revolution, but they've got us thinking... When you combine spontaneous, inconspicuous video with face recognition and AI, well, who knows what you could do? The premise is simple: wear Specs, click to shoot, share on Snapchat (or not, you choose). Specs let viewers truly see the world through your eyes. But beyond that, Spec's camera lenses could reinvent computing the way the keyboard and mouse or touchscreen already have. Computers now recognize images: type of bird, location in Yellowstone, person in your video, etc. Practical or not, these glasses make sharing your world easy and fun.

-Wired

For Sale: DDoS attacks from 400,000 IoT devices.

Got a journalist you'd like to punish? A core chunk of Internet you'd like to take down? A sovereign nation you'd like to knock offline? As of a couple of months ago, you could rent your own time on the Mirai Worm, a botnet that took down Level 3, Twitter, Dyn and other hardened, well- provisioned Internet giants, and spread to every developed nation on earth last October. Two criminals, BestBuy and Popopret, previously implicated in mass-scale corporate espionage, have run ads for this service. Typical price? Three to four thousand dollars per two-week attack. Can they deliver? Given that most IoT devices are poorly protected, and the Mirai botnet has loads of room for improvement, don't count them out.

-BoingBoing.net