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

Readiness Test

Brave enough to test your cyber defense? Think your network is hacker proof? We have a way for you to put your reputation on the line without paying a dime to any cyber criminal.

We've partnered with one of our detection security firms to offer a limited time, FREE scan www.secureerpinc.com/cyber-threat-assessment It's impossible to manage a risk you haven't measured and it's FREE. There's no better time.

March 2021

Too many businesses are exposed and vulnerable to cyber attacks. With a unique Guardian Angel Protection solution, our clients get back to their business and sleep better knowing their data is secure

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

3 Questions You Should Ask Any IT "Expert" Before Letting Them Touch Your Computer Network

There are seemingly countless IT services providers to choose from these days, and it can be challenging to tell one from another. However, not all IT services providers are created equal. Some offer independent services, while others are part of larger firms. Some are new to the field, while others have been around for years. There are also companies that put out slick marketing to grab your attention but make it hard to tell if they really live up to the hype.

Well, we're here to help you cut through the clutter. You want to hire someone who knows what they're doing and will take care of your business the right way. To do that, there are a few questions you should ask every IT expert before you let them anywhere near your network – to ensure you'll be in good hands.

1. **What's Your IT Experience?**
Education, certifications and hands-on experience are all important. You want to know your "expert" is actually an expert. It's all too easy for someone to pass themselves off as an expert when they really have limited experience, so you should never hire an individual or a company without vetting them first. After all, this person (or team) will be handling EXTREMELY sensitive hardware and data essential to the operation of your business. This isn't the time to take risks or give someone the benefit of the doubt.

When you work with an IT services company, or MSP, you can generally expect that the people you work with are educated and experienced, but you should **always** ask. It's okay to dive in and ask them about their certifications, how long they've been doing their job and how familiar they are with your industry. And if you aren't sure what

Continued on pg.2

Continued from pg.1

certain certifications are, feel free to ask follow-up questions. There's a very good chance they'll be more than happy to answer all of your questions, especially if they're a true professional who knows what they're doing!

2. **What's Your IT Approach?**
There are different approaches to IT and network security. You have the old-fashioned **break-fix** approach and you have the modern **proactive** approach. The break-fix approach used to be the staple of the IT industry – it was the business model of just about every IT support firm in the 1990s and early 2000s. This approach is pretty straightforward: something breaks, so you hire someone to come in and fix it. If many things break or something complicated breaks, you could be looking at a pretty hefty bill – not to mention the costs associated with downtime.

Today, most MSPs take a proactive approach (and if they don't, look elsewhere). They don't wait for something to break – they're already on it, monitoring your network 24/7, looking for outside threats or internal issues. They use advanced software that can identify trouble *before* it strikes. That way, they can go to work, proactively protecting your business so you avoid those hefty bills and long downtimes. These are companies that are willing to collaborate with you and your business to make sure you're protected, your IT needs are met and you're getting your dollars' worth.

"If you're working with an IT company that doesn't have your full confidence, you may need to rethink that relationship."

3. **What's Your GUARANTEED Response Time?**
This question often gets overlooked, but it's one that can make or break your business – and it can make or break your relationship with your IT services provider. You need to know that you won't be left in the dark when something goes wrong within your network. If you're experiencing a cyber-attack, or a power surge has taken out part of your server, the cost to your business can be catastrophic if your IT services provider can't get to you right away. The longer you have to wait, the worse it can get.

You need to work with someone who can give you a guaranteed response time in writing. It should be built into their business model or, better yet, the contract they want you to sign when you hire their services. They should be doing everything they can to instill confidence that they'll be there for you when you need them. If you're working with an IT company that doesn't have your full confidence, you may need to rethink that relationship.

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
www.secureerpinc.com/protect
or call our office at (317) 290-8702.

Cyber Security TIPs

Ransomware works by encrypting your files to prevent you from accessing them. The hackers behind the attack then pop up a demand screen asking for payment within a set time frame (e.g., three days) in order to get the key to decrypt your files. Ransomware has forced many business owners to lose data or pay up since there was no other way to decrypt the files – and many paid without getting their files back.

Obviously the best way to foil a ransomware attack is to be incredibly diligent about IT security; but **with nearly one million new attacks being created daily, there are no guarantees that you won't get infected**. Therefore, it's critical to maintain a full image-based, not just daily, but continuous backup of your data OFF-SITE so that IF you do get whacked with ransomware, you can recover all your files without having to pay a thin dime– AND your backup needs to be a professional-grade backup that is impervious to ransomware since hackers write their attacks to infect BOTH your PC/server AND your backups. Will your backup survive? MANY DON'T.

We'll review your current backup strategy with a Business Continuity Assessment in a 10 minute Zoom call. - R²

Making & Keeping Customer Connections In A Digital Era

Make the value that you give your customers so high it doesn't matter what the price is. Based on the experiences your brand consistently delivers, your customers should have no idea what your competition charges. You don't need to raise your prices. You need to bring value and better service. This includes employee training – and be sure they understand how to build and keep relationships.

3 Strategies To Dominate The Relationship Economy

- Use technology to allow employees to focus on what's most important: building relationships that result in higher customer loyalty.
- Build a culture that creates emotional connections with your employees.
- Create relationship-building training for new and existing employees.

Things That CAN Be Trained:

- Authenticity
- Insatiable curiosity
- Incredible empathy
- Great listening skills

The 1 Thing That CANNOT Be Trained:

- The ability to love people

Let's focus on what can be trained and what these traits look like.

Authenticity:

- You love what you do, and it's obvious.
- You're transparent – if you have bad news, don't hold it back.
- You are as committed to the success of your customer as they are.
- You know your clients' top three goals for the year.
- Your customer should not be able to imagine a world without your business in it.

Insatiable Curiosity:

- You're dying to learn about others.
- You want to know about both familiar and unfamiliar subjects.
- You're willing to meet as strangers but leave as friends.

Incredible Empathy:

- You look at things from the customer's perspective.
- You put yourself in your customer's shoes.
- You listen and think from the other person's point of view, allowing their message to become much clearer.
- You're wary of empathy fatigue and able to reset yourself.

Great Listening:

- You give them fierce attention.
- You ask a question and then more questions.
- You don't defend questions and instead explore new ones.
- You bounce questions back.
- You fight the urge to reply before you finish listening.

Every employee should possess these four traits, and you should be willing to train your team to deliver on these traits. When you successfully bring these four elements together, you are set up for success and have the foundation to build and maintain strong relationships with your customers.

Leah Tobak is a Project Manager with Petra Coach. With a background in public relations and marketing, she's done a lot of work building relationships with customers and prospective customers. Outside of the corporate landscape, Leah is an international model and is known for her work in front of the camera.

Top 4 Security Certifications You Should Have In 2021

GIAC Security Essentials (GSEC)
Ideal for those who may not have an extensive background in IT security and networking but who work in an IT security (or similar) role and want a baseline certification. No prerequisites. Learn more at **GIAC.org/certification/security-essentials-gsec.**

(ISACA) Certified Information Security Manager (CISM)
Less technical and more managerial. Ideal for those in IT and risk management roles that are not strictly technical. Prerequisites for certification include five years experience in information security (including three years as an information security manager). Learn more at **ISACA.org/credentialing/cism.**

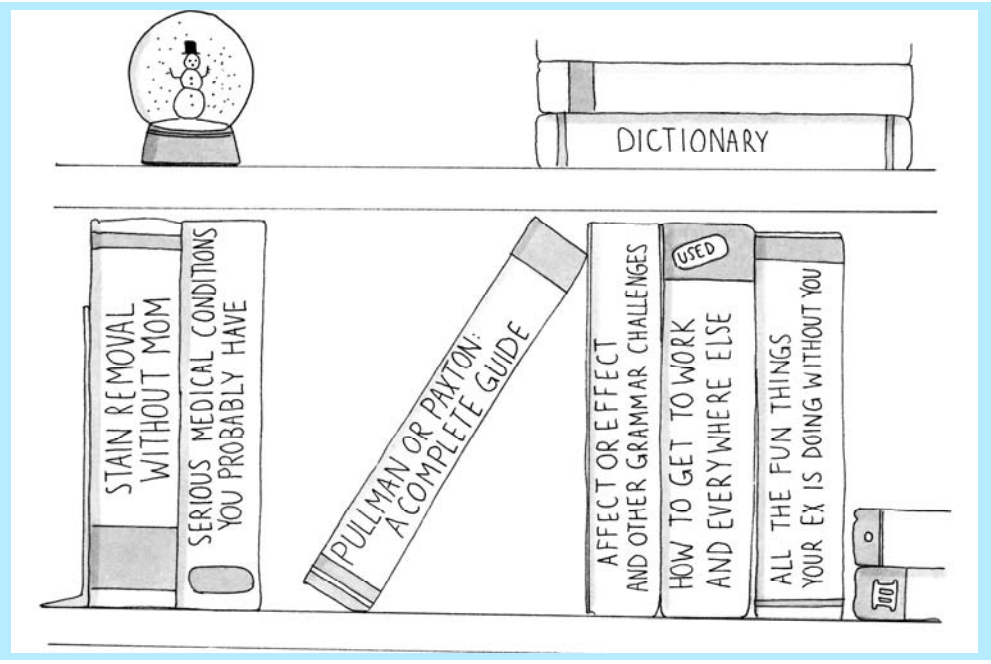
(ISC)² Certified Information Systems Security Professional (CISSP)
A high-level certification aimed at those with an extensive and knowledgeable IT security background. This certification is in very high demand by companies around the world. Prerequisites include five years experience in a position related to CISSP (or one year of experience plus a four-year degree). Learn more at **ISC2.org/certifications/cissp.**

(ISC)² Certified Cloud Security Professional (CCSP)
Ideal for those experienced in IT security with an emphasis on cloud-based solutions. Prerequisites for certification include a minimum of five years of full-time IT experience (with three years in information security). Learn more at **ISC2.org/certifications/ccsp**.
Infosec, Dec. 22, 2020

The Scientific Reason Your Employees Value Opinions Over Facts

The research is clear: people have a habit of putting more value on opinion rather than fact. It's because it's easy! This is discussed in Daniel Kahneman's best-selling book, *Thinking, Fast And Slow*, and in numerous research papers. Accepting opinions requires less thinking than evaluating facts. Data-driven companies need to take this into account when it comes to their teams. According to Kahneman, some people are "type 1" thinkers or fast thinkers, and opinions mean more to them. Others are "type 2" or slow thinkers – they take their time and evaluate what they hear.

Michael Schrage, research fellow at MIT Sloan School's Center for Digital Business, says you can't just switch between the two types of thinking automatically. It's more fundamental – you have to change people's mindsets over time. His suggestion is to incentivize analytical, fact-based thinking and recognize employees who take this approach. *Inc., Oct. 29, 2015*



3 Simple Yet Effective Ways To Boost Employee Morale

1. Focus On Mental Health. Whether it's your own mental health or the mental health of anyone on your team, make sure everyone has the time and space they need to take a break and refocus their energy. Make sure anxiety and stress are recognized and addressed in a positive way.

2. Be With Your Team. Simply being present and available for everyone on your team goes a long way. Have regular one-on-one chats just to see how things are going and to ask if they need anything. When they do need something, do what you can to help (and be sure to follow up).

3. Recognize Your Employees. Recognize their work and reward them. Everyone should be aware of the effort individuals and teams put into their work. At the same time, make sure they have ownership over their work and give credit where credit is due. *Inc., Nov. 4, 2020*