Cyber Times

Newsletter by Secure ERP, Inc.

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

Dark Web Stolen Credential Monitoring

Using proprietary technology, our monitoring service searches the most secretive corners of the dark web to find your company's stolen credentials (email and password) for sale to criminals. We not only alert you when this happens, but also work with you to mitigate the risk this poses to your company. This is an invaluable early warning red flag that your risk of a breach may increase without an adequate response.

Don't take that chance!
Learn more: secureerpinc.com/dark-web-monitoring or call us at (317) 290-8702 for a demonstration.

Guardian Angel Dark Web Monitoring BY Secure ERP, Inc

October 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.

Skimp On Data Protection And Pay The Price

We've said it time and again: Today's cybercriminals are using more advanced technology than ever. And those malicious tools are becoming even *more* sophisticated at a breakneck pace. To top it all off, new software developments are enabling these criminals to cast wider and wider nets, targeting businesses that, before, would have flown under their radar. Companies small and large, of every type, are being infiltrated by vicious cyber-attacks across the world each and every day.

Even knowing this, business owners are tempted to cut costs and corners. When you've never had a breach, data security can seem like a distant concern, especially for a limited budget. But regardless of which digital barriers you put in place to protect your business, you can bet on one thing: One day, your security will be tested by an attack. Whether or not the hackers punch through could mean the difference between your company shutting down for good — as 60% of small businesses do in the six months following a cyber-attack, according to the *Denver Post* — and remaining solvent and secure in your position.

When you're struggling to stay afloat or simply wanting to be a savvy spender, you may think the best way to lock down your data is to put one of your staff on the task or to do it yourself.

continued on pg 2

...continued from cover

And sure, your team can conduct hours of research searching for inexpensive security. And you'll almost certainly find something cheap with good reviews and a decent track record. You'll figure out how to install the software across your system, complete with firewalls, server protection, antivirus and maybe a bell and a whistle or two. Perhaps you'll even hold a meeting to educate your staff on the do's and don'ts of cyber security. "Use intricately constructed passwords," you'll tell them. "Don't click suspicious links in your email."

"Cyber security is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses," wrote the Securities and Exchange Commission in a 2015 report. "The reason is simple: small and midsize businesses are not just targets of cybercrime; they are its principal target."

Then, after a few days of fiddling with settings and ensuring the security software is properly in place, you'll forget about it altogether. After all, it's already installed, and you've checked to make sure there aren't any gaps in the system. It's not something you need to constantly monitor.

A year later, your business has — miraculously — doubled in size. You're finally reaping profits. Best of all, a recent news story has brought your company into the public eye, and brand-new leads are contacting you every day. For the first time since the company's inception, you can breathe easy.

Then, one Monday morning, you log into your computer. For a second, everything seems to be normal, until an innocent-looking pop-up fills your screen. "Attention!" an eerie robotic voice barks from your speakers, "Your documents, photos, databases and other important files have been encrypted!"

Thinking it's a hoax, you click into your server drive. To your dismay, you really are locked out of everything. So, palms sweating, you read the rest of the pop-up. It provides instructions to install the deep web browser Tor as well as an address for you to visit. When you go there, you learn that in order to recover all your data, including the credit card information of your customers, you'll need to dish out $50,000 in bitcoin.

A year ago, you couldn't afford adequate cyber security. Can you afford $50,000 in cash today?

Identical situations are unfolding every day, with people *exactly like you*. Back in April, CNBC reported that across the previous 12 months, *half* of all small businesses had been infiltrated by malicious hackers. "Cyber security is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses," wrote the Securities and Exchange Commission in a 2015 report. "The reason is simple: small and midsize businesses are not just targets of cybercrime; they are its principal target."

Cheapo security solutions might be fine for a lone browser surfing the web at home, but they are shockingly inadequate resources on which to base the entire success of your company, your livelihood and the livelihood of your employees.

Frankly, it's irresponsible to lock your data behind a flimsy $5 firewall. Invest in robust cyber security solutions and secure the future of your company.

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 unanticipated costs.

Claim Your FREE Copy Today At www.secureerpinc.com/itbuyersguide Or Call Our Office At 317-290-8702.

Cartoon Of The Month

"Tom, as your legal counsel I feel I'd be remiss if I didn't recommend against this one last time."

...continued from page 4

encrypts all the local files, making them unlockable only with a private key held by the attackers. Attackers then demand exorbitant sums of Bitcoin in order to recover the data — or threaten to make it inaccessible forever. The strategy has proven highly profitable for cyber-criminals, who have adopted it in droves. Just this summer, San Francisco's largest public radio station was hit by ransomware, forcing employees to rely on mechanical stopwatches and paper scripts in the aftermath.

Additionally, it's clear from the data that ransomware designers are constantly developing more and more ways to penetrate antivirus software. When antivirus identifies a specific malware program, the system usually scans for matching binaries. But modern ransomware is able to change its binary once it has been detected, allowing it to skate past many outdated defense systems. *TheVerge.com 7/25/2017*

Password Management As An Employee Benefit

With everyone's life increasingly being impacted by stolen data, as in the Equifax breach, your passwords are more critical than ever before. It's the same for your employee's personal passwords too!
What if you could offer them the **FREE** employee benefit of securely storing all their personal passwords, which NO ONE ELSE would be able to access?
Your business has taken cyber security seriously and been mindful of protecting your data. You've invested in firewalls, anti-virus, spam filtering and backup/disaster recovery tools. But when was the last time you considered the first line of defense beyond all these security measures? Passwords are used to protect your systems, data and online accounts; however, the difficulty of remembering strong passwords often puts people off from creating them.
Now you can accomplish both in a way that's affordable and increases your cyberprotection on a basic level.

Learn more at secureerpinc.com/password-management-as-a-service/ or call our office at **317-290-8702.**

Are Your Clients Sucking The Life Out Of You?

Bad clients aren't just a nuisance, they're bad for business. They can take an inordinate amount of time to service. They may complain about irrelevant details, avoid paying their bills or drag payments out forever. They can be a huge emotional drain. Or, more often than we care to know, they can do all of the above.

Firing these bad apples can be an attractive option. But what if that client is buying a profitable product from you? What if they're 60% of your revenue? Firing them will eliminate a big headache, but it may also put you out of business.

Not all clients are created equal. When you're considering a "keep 'em or kill 'em" approach, take these steps first.

1. CONDUCT A CLIENT ASSESSMENT
Assess your problem clients, considering factors like their historical revenue, projected future revenue, their core values and other indicators. Keep in mind, if a client was the ideal client before, you may be able to nudge them gently back to their former selves.

2. REMIND THEM WHY THEY DO BUSINESS WITH YOU
To you, a problem client is nothing more than a pain in the neck. But to them, your business obviously has redeeming qualities that keep them working with you. Schedule a meeting with the client and explain the challenges you are facing with them. Ask them if they'll make the commitment to improve. It may be an awkward situation, and they may say no, but either way, the conversation can't make things worse.

3. MATCH PERSONALITIES
Sometimes, business difficulties are nothing more than a personality mismatch. If you're consistently having trouble with the same employee, ask the client if they can assign a new liaison from the company. Even if you're dealing with the boss, they may be willing to let you work with one of their employees or colleagues instead.

4. LAY DOWN THE LAW
This is one of the toughest parts of being a vendor, but it's critically important. You need to clearly outline the rules of what is or isn't acceptable. Meet with the client and tell them exactly what is wrong, exactly what they need to do to fix it and exactly what the consequences will be if they don't.

5. SET A STOP LOSS
Once you've tried addressing the issues you're having with the client, put a deadline by which your suggested changes must be implemented. Plan and commit to the action you will take at that time, depending on what the client does.

6. GET OUT OF THE TRAP
If nothing fixes the problem, yet you decide to continue the relationship, you need to realize the problem is not the client's, but yours. There is something in your actions that indicates you are willing to be treated the way they are treating you. It's unlikely that they'll stop. At this point, your best bet is probably to bite the bullet and fire the client once and for all.

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, a consulting firm that ignites explosive growth in companies that have plateaued; 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 www.mikemichalowicz.com/

6739 Cobden Lane
Indianapolis, IN 46254

Inside This Issue

Use Technology To Boost Your Bottom Line

As technology progresses at a breakneck pace, it's improving the modern workplace in turn. Regardless of the size of your business, technological developments can bolster your team, your customer's experience and the success of your company overall. The possibilities are endless. Use time-tracking software to see the bottlenecks in your company's day-to-day and streamline your processes. Utilize social media technologies to drastically improve your marketing. Deploy machine learning to provide better automated customer service. If you're not staying abreast of the latest advancements, you're putting yourself at a steep disadvantage to your competitors. *SmallBizTechnology.com 5/2/2017*

NO CASH? NO PROBLEM, WITH THESE HANDY PAYMENT SERVICES

These days, if a friend covers you at the restaurant, you have no excuse not to pay them back immediately — assuming you're good for it. Between Venmo, Square Cash, Apple Pay, Facebook, and more recently Gmail and even Skype, there are numerous digital payment services that enable you to send money at the touch of a button. Skype's entry into the field, particularly, is useful for international payments, covering 22 different countries. *Lifehacker.com 8/6/2017*

IF YOU'RE NOT A FAN OF HUMAN INTERACTION WHEN IT COMES TO YOUR INSURANCE CLAIMS, THIS IS GOOD NEWS

The increasingly digitized world means a growing number of interactions between people and machines. According to a 2017 survey by LexisNexis, insurance companies have been looking into virtual or "touchless" methods of handling claims. A full 38% of insurers said they won't be sending human employees for physical inspections at all in the future, instead using drones or apps. *DigitalTrends.com 8/8/2017*

OVER $25 MILLION IN "RANSOMS" PAID OUT IN JUST THE LAST TWO YEARS DUE TO RANSOMWARE ATTACKS

According to a study presented by Google last July, ransomware victims have paid out more than $25 million in ransoms over the last two years. Ransomware is a viral program that, after infecting a system,

continued on pg 3