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

Join Us

Be my personal guest as I sit on the discussion panel with other cyber security experts to discuss your business concerns.

Register Online:

http://bit.ly/bankatfirst-feb20

February 2019

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 and Cybersecurity Evangelist, Secure ERP is dedicated to protecting our clients' data and supporting their people and growth.

Why Your Business Is The PERFECT Target For Hackers

Is Your Protection Up To Date?

People never think it'll happen to them. Sure, they see the reports – 50 million-plus bundles of user data compromised by a Facebook breach; the billing information of more than 2 million T-Mobile users hacked by a mysterious malicious entity – but companies like those are massive, monolithic entities in American commerce. They're decidedly big fish, not like *you* and *your* small business. According to a recent JLT-Harvard Business Analytic Services survey, more than half of small business owners remain locked into this line of magical thinking, blissfully unaware of the threat cyber crime poses to the health of their organization.

We hate to burst the bubble of the happy-go-lucky majority, but the reality is that this optimistic attitude just does not square with the statistics. The incidents may not make the news, but small businesses are being targeted – and breached – by hackers at an astounding rate. In fact, the National Cyber Security Alliance reports that close to half of small businesses have experienced a cyber-attack and that 60 percent of the companies that succumb to one of these attacks folds completely within six months. They state that instead of zeroing in on Fortune 500 corporations, hackers actually prefer to swoop in on the little guy, with 70 percent of cybercriminals specifically targeting small businesses.

Yet according to a Paychex survey, 68 percent of small business leaders aren't worried about cyber security despite data from Hiscox indicating that more than seven out of ten small businesses are woefully unprepared for a breach.

Continued on pg.2

Continued from pg.1

Of course, it's understandable that the average small business owner shirks their cyber security responsibilities. It's the kind of problem that's so complicated that it's tempting to sweep it under the rug. As breach tactics become more sophisticated, so do the softwares and methodologies designed to keep out criminals. In a world far removed from the days when buying a product and installing it into your network was enough, it's easy to become overwhelmed by the complexity and breakneck pace of advancing cyber security best practices. Our biases make the possibility of a hack seem remote, while our limited resources make the cost of protection appear too high to even consider.

The first step to getting savvy in 2019 is to accept that cyber-attack isn't some unlikely crisis, but a virtual inevitability. It's a tough pill to swallow, but leaving it to chance is like flipping a coin where a "tails" outcome results in your business shuttering for good.

Luckily, though an attempted hack is almost guaranteed, there are dozens of steps you can take to prevent it from doing any damage. Chief among these should be to find a managed service provider (MSP) with a long background in protecting against hacker threats to take the reins on your cyber security as quickly as you can. It's important when auditing your internal security measures that you regularly get an outside opinion from a trusted source, in order to cover all your bases. Your internal IT departments assurances that "they've got it covered" are certainly reassuring, but to truly patch all the holes in your security barriers, you'll need more eyes on the problem. You might imagine that such a partnership must be prohibitively expensive, but they're typically more reasonable than you might think. Not to mention that when the very survival of your business is on the line, it just makes sense to budget accordingly.

> **"The first step to getting savvy in 2019 is to accept that a cyber-attack isn't some unlikely crisis, but a virtual inevitability."**

The statistics paint a picture of small business owners as underprepared, unaware, and disturbingly vulnerable to the whims of cybercriminals hiding just out of view. Don't be another one of the millions of small business owners forced to shell out thousands as a consequence of wishful thinking. Wake up to the dangers of 2019, arm yourself against them, and secure the future of the business you've worked so hard to build.

Cyber Threats & Solutions Webinar Series

Thursday, Feb 21 @ 1pm EST—The Travel Edition

When you're traveling you're at greater cyber risk than in the office.

Who Should Attend? C-Level executives & managers who are concerned about lost or stolen devices; privacy of confidential information; employment litigation introduced when employees use personal devices to access company data; and reputational damage along with State & Federal laws that carry heavy fines for lost or stolen customer/employee data. Of particular importance for those organizations that handle ANY sensitive data, medical records (or serve clients who have such records) or that want to avoid having their bank account wiped out due to a cyber-attack or ransomware.

Register online: https://events.genndi.com/channel/secureerp21feb
or call our office at (317) 290-8702.

Our passion is your cyber protection, worry free tech is what we deliver.
www.secureerpinc.com • (317) 290-8702

Cyber Security TIPs

FBI Warning of Direct Deposit Scam

Reported on the FBI's Internet Crime Compliant Center (IC3) found on www.ic3.gov this is a new twist on social phishing. Here's how it works:

Cybercriminals target employees through phishing emails designed to capture an employee's login credentials. Once obtained, the credentials are used to access the employee's payroll account in order to change their bank account information. Rules are added by the cybercriminal to the employee's account preventing the employee from receiving alerts regarding direct deposit changes. Direct deposits are then changed and redirected to an account controlled by the cybercriminal, which is often a prepaid card.

The FBI lists several mitigation steps with the first being education. Training employees to spot and avoid phishing attacks stops the scam before it starts. Implement a security training program with simulated phishing attacks for your employees. It costs less than you think and is just smart business. We'll help you organize it.

When Service Becomes A Disservice

Today is a tough time to be a bookseller. Whether you're a local, independent bookstore or a chain mega-giant, the online market is putting the squeeze on your bread and butter. Personally, I want bookstores to succeed despite the new digital world. I always prefer brick-and-mortar to digital.

For that reason, I'm a longtime fan of Barnes & Noble. There's one near my office that I visit frequently to check out new arrivals and figure out what to read next. But lately, something's changed. In the past, it could be difficult to find someone to help me around the store. Today, it is difficult to avoid someone trying to help – whether I want them to or not.

Today's Barnes & Noble stores usually have an employee waiting for you at the front of the store. They ask what you're looking for, and if you're like me, you reply, "Oh, nothing, just looking." This spurs them to belt out a spiel about specials and book recommendations. It can be off-putting, to say the least, and it's the perfect example of when service feels less like help and more like a hustle.

Successful businesses always guide and sell to their prospects, but customers don't want to feel pressured and pushed. How can you tell when you've crossed the line? It's a vital question for anyone who wants to provide exemplary customer service.

I believe there are four tiers of poor service:

1. Avoidance. Employees aren't visible or easily identified, and you have to hunt them down.

2. Apathy. You can find employees, but they seem at worst annoyed by your questions and indifferent at best. They're just going through the motions.

3. Assertiveness. Employees initiate contact both by greeting customers and offering to help. "How may I help you?" is the classic phrase. If the customer responds with, "Just looking," all that's needed in response is, "Please let me know if I can be of any assistance." No pressure.

4. Aggressiveness. Employees engage with everyone who comes in, regardless of the customer's receptivity or lack thereof. They assume you know what you want and ask what it is. When you try to get them off your back, they launch into a sales pitch.

We all like employees who are knowledgeable, friendly and eager to help. But too much enthusiasm turns service into a disservice. Skip the canned sales pitches and only guide customers who are looking for your help.

Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the bestselling author of books like Fred Factor *and* The Potential Principle *and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.*

3 Ways To Protect Your Business From Cyber-Attacks

1. Plan for the worst.
The sad truth is that, no matter how much most businesses prepare their defenses for a cyber-attack, a breach will often occur anyway. That doesn't mean you shouldn't invest in protection, but you should always have a plan in place if and when crisis strikes. Include actions to contain the breach, patch the affected systems, and coordinate teams (not just IT) to stay on top of the problem.

2. Keep your team in the know. The vast majority of breaches are instigated through minor errors by everyday employees. These noncompliant security behaviors aren't just bad for your business; they're bad for PR. That's why cyber security should be everyone's priority, not just the techies in your business. That means educating everyone on what to watch out for and what to do when hackers come knocking at your door.

3. Budget for robust cyber security.
Of course, all of these measures won't mean a thing if you don't actually invest in cyber security. Instead of a one-and-done task to check off, cyber security actions should be a regular component of your day-today. Include the costs of training, employee time, documentation, consulting and the latest security innovations.
Smallbiztrends.com, 11/20/2018

5 Mistakes Leaders Make That Keep Their Companies From Growing

1. Becoming complacent. No matter how comfortable the status quo is, stagnation only leads to failure down the road.

2. Pouring money into a failing project. When a venture fails, it's best to learn from it and move on rather than dump more resources into a clunker.

3. Entering a new market without the requisite knowledge. Don't overreach – only expand your business's focus when you really know what you're getting into, inside and out.

4. Focusing on the short-term. Never take an immediate win that will jeopardize long-term success.

5. Succumbing to analysis paralysis. Overthinking is fatal. Stay nimble and informed, but don't let it stop you from actually acting.
Inc.com, 11/8/2018