TECHNOLOGY TODAY

High Hopes!

We're beaming with pride that our CEO, Yuri Aberfeld, has been nominated for Ernst & Young's "Entrepreneur of the Year" award! We're crossing our fingers and looking for ways to rig the voting… (Oops! Did I actually write that out loud?)

Because of the unique business model he's built here, positioning IT Support LA as 'Technology Concierge', handling every aspect of office communication, including managing other vendors, we think he should be a shoo-in.

But just in case, he's practicing his Academy Award style *'I lost, but I'm sooooo happy for the winner'* smile.

March 2019

This monthly publication provided courtesy of Yuri Aberfeld, CEO of IT Support LA.

IT Support LA creates the possibility of focusing on business goals and priorities by providing a trusted technology partnership to small businesses.

3 Ways Your Employees Will Invite Hackers Into Your Network

… And What You Must Do To Prevent It TODAY

No matter how professional they are, members of your team – yourself included – are going to make mistakes. It's true of every organization on earth. They'll spill scalding coffee into the company copier. They'll work overtime until the office is empty, then head home without thinking to arm the security system. They'll neglect key accounts, muck up workflows and waste hours developing convoluted solutions to simple problems. And, worst of all, they may unknowingly bumble into the cyber-attack that forces your business to go belly-up for good.

In the majority of cases, that will be by design. There's a saying in the cyber security industry, coined by renowned cryptographer Bruce Schneier: "Only amateurs attack machines; professionals target people." When it comes to repeating the same process safely and autonomously, machines are less fallible than the average person sitting at a desk. Savvy hackers looking to boost funds from unsuspecting small businesses know this. So instead of developing a complex program that dances around the security measures baked into sophisticated modern technology, they target the hapless folks on the other side of the screen.

The strategy works disturbingly well. According to IBM's 2018 X-Force Threat Intelligence Index, more than two-thirds of company records compromised in 2017 were due to what they call "inadvertent insiders" – employees who left the front door wide-open for the bad guys without even realizing it. Negligence, lack of awareness and sheer bad luck put the best-laid plans to shame on both sides.

But how does it happen? There are three primary causes of employee-related breaches, each of them contributing to a sizable portion of hacks across the country.

Continued on pg.2

Continued from pg.1

1. SOCIAL ENGINEERING

Phishing remains one of the most prominent strategies deployed by hackers to lift data from small and midsize businesses. The majority of these attacks stem from an employee clicking on a suspicious link that is embedded in a dubious or absolutely convincing e-mail. To lure your team into the trap, cybercriminals often use data gathered from cursory investigations of your organization from the Internet or social media. Maybe they pose as a security expert contracting with your company or a member of a customer support team behind one of your employees' personal devices. Whatever mask they wear, it doesn't take much to convince an uninformed individual to click on anything at all, resulting in a high success rate for phishing attacks.

2.CIRCUMVENTED OR INCORRECTLY IMPLEMENTED SECURITY MEASURES

Even if you do everything you can to protect your business from digital attack, your team may just dodge those measures anyway. According to a report by cyber security firm Dtex Systems, around 95% of companies have employees who will attempt to override previously implemented security processes. And that's if the security measures are configured, patched and installed properly in the first place. The IBM X-Force report lists "misconfigured cloud servers and networked backup incidents" among the chief concerns of last year.

> **"Negligence, lack of awareness and sheer bad luck put the best-laid plans to shame on both sides."**

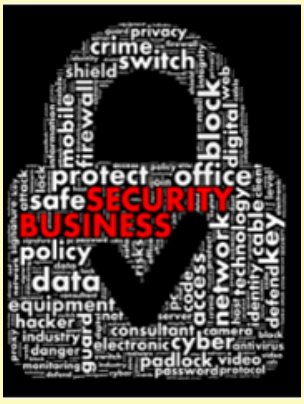
3. INSIDERS WITH MALICIOUS INTENT

Hell hath no fury like an employee scorned. A strikingly large number of breaches come not from error at all, but from insidious tactics by disgruntled employees or undercover criminals looking to make a quick buck. It's not quite a "you can't trust anyone" scenario, but there are definitely folks out there who would sell your business right out from under your nose.

With each of these in mind, it's vital that you incorporate extensive employee training and vetting protocols to maximize their cyber security know-how. In addition, you need to implement safe practices that reduce the room for human error, alert employees when something is amiss and protect them from the worst.

We can help. It's difficult to overhaul your cyber security, especially on the people side, without a round-the-clock team dedicated to pinpointing the weaknesses in your organization and working to patch them up. In 2019, human error is poised to take an even more central role on the stage of digital crime. Don't leave it up to chance.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now



At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call our office at 818-797-5300.

Donkey Con

Say it ain't so! Crafty criminals are including a PowerShell command in the pixels of images of Mario, the hero of Donkey Kong from Super Mario Bros. This is only the first in a series of attacks that employs the pixels of innocent looking photos and graphics to carry malware into your system. This type of attack slips by typical malware protections and throwing a barrel at it won't solve the problem.

So let's say you get Ransomware – as we've always said: it's not a matter of IF, but of WHEN, and now someone in your office can receive an email containing what looks like a funny graphic – except it's too small to read, so they download it and BOOM – your system locks up and you have no access to your company data.

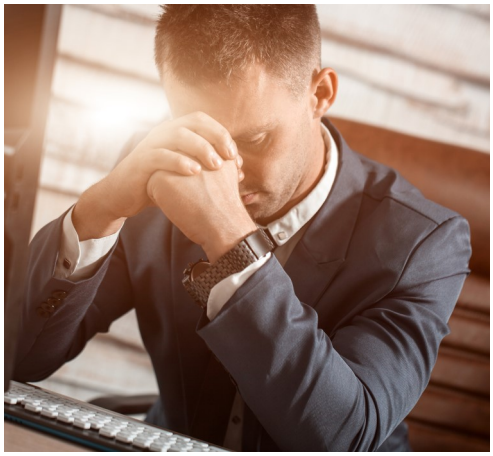
NOW what do you do? If your small business has a 'typical' IT guy who just keeps patching together your system, you are going to need a good Data Recovery company. This is where they hit you twice. There are shady Data Recovery companies working hand-in-hand with GrandCrab a prolific malware distributed through numerous Ransomware 'exploit kits'. It's like having a fire at home, but the firetruck that shows up works for the arsonist!

When Ransomware happens, look for a company that is known, whose name you have at least heard of. Here at IT Support LA, we have rescued many companies from paying a ransom, but only when we have something to work with: reliable backups. Our clients have them, do you?

For a FREE assessment of your security measures and the reliability of your backup systems, either call us at 818-797-5300 or go to www.itsupportla.com/free-stuff/free-network-security-assessment/

Still Not The Person You Always Wanted To Be?

3 Steps To Get You There In 2019



We all aspire to be better people, but too many of us hesitate to roll up our sleeves and tackle the roadblocks that prevent us from achieving that goal. We stay in our comfort zones, fall back on old habits and then question why our life isn't improving.

When I'm coaching CEOs and they tell me they're stuck in a rut, I always have the same response: start changing what you are doing in your life, because the person you are today will not get you to where you want to be.

Here are three guidelines to do exactly that.

1. START BY GETTING FOCUSED.
When planning any journey, the first thing you need to know is where you are. In business, you hold monthly and quarterly meetings to review operations and financial statements so you know how the company is doing. You should be doing the same thing for yourself.

Then you need to figure out where you want to go. What do you want your life to look like one, two or three years down the road? Map out specific goals to achieve this, and then follow them religiously. Stay on task, but don't multitask. Limit your distractions, and control your time.

2. WRITTEN, MEASURABLE GOALS ARE A MUST.
The first and most important step toward achieving and exceeding your goals is to write them down. I cannot stress this enough. Writing down your goals and priorities serves as a reminder of what you need to accomplish. As much as you can, keep them SMART: specific, measurable, attainable, relevant, and time-bound. Carry your list around with you and act on it every day. Do it for 30 days, and you'll be amazed at your progress.

3. LAY A FOUNDATION FOR EXECUTION EXCELLENCE.
If you've ever played sports, you are probably familiar with the phrases "in the zone" or "in the flow." It applies to any profession, from songwriting and acting to computer programming and engineering. When you're in the flow, you feel good, have a ton of energy and get a lot of work accomplished. Find the things you need to do on a daily basis to stay in the flow – whether that's exercise, meditating, reading or anything else – and write them down.

It's also essential that you hold yourself accountable along this path. Find an accountability partner and share with them your tasks, priorities and deadlines to accomplish your goals. You are much more likely to succeed when you have someone watching your progress and ensuring you cross the finish line.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

4 Steps To Protect Your Business After The Marriott Data Breach

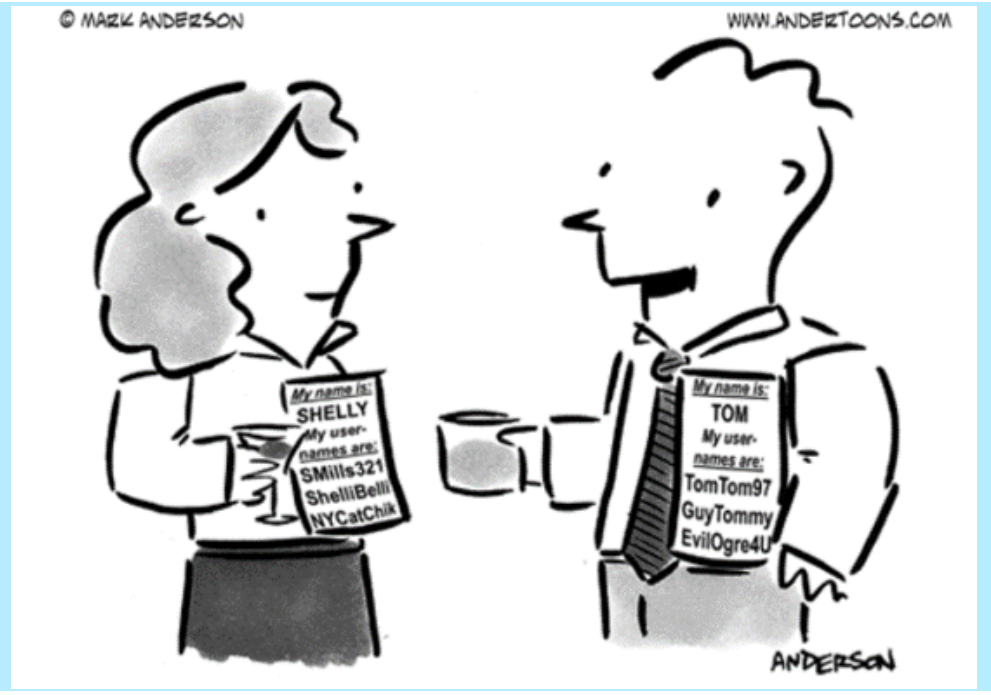
Last November, Marriott announced some bad news: the data of up to 500 million customers may have been compromised in an attack. If you travel regularly for business and are a customer of the Marriott chain –including Westin, Sheraton, the Luxury Collection, Four Points, W Hotels, St. Regis, Aloft, Element, Tribute Portfolio and Design Hotels – there are some things you need to do.

First, change your passcodes. This should include your potentially compromised account and any accounts that, for some reason, still use the same login or passcode in 2019. Then, start keeping a close eye on your credit card and bank accounts. You may even want to consider freezing your credit. Finally, be very careful about opening e-mails. Cybercriminals love piggybacking on actual customer contacts from big corporations to send out phishing e-mails. *SmallBusinessTrends.com, 12/13/2018*

3 Ways To Turn Your Culture Into A Competitive Advantage

It's easy to focus on metrics like profit and market share when you're working to succeed. But when you fixate on these numbers instead of the people in your organization, folks start to feel like nothing more than cogs in the machine.

According to a recent study by FTSE Russell, all the companies that have received the prestigious "FORTUNE 100 Best Companies to Work For" have a single thing in common: keeping employee experience at the top of their list of priorities. These companies have stock market returns up to triple than the market average and lower turnover rates than their competitors.



But what does turning your organization into one where "employees come first" actually look like? The first step in this massive undertaking is to pick a "champion" who understands the goals of the project and the value of their team. Then, they can begin to assess where the problems are in areas like your mission, transparency, trust, communication and core values.

Soon they'll enlist the team on the project, creating regular rituals that reinforce your budding company culture. After a firm, long-term commitment to a new culture, you'll find your company, and the people who drive it, to be healthier than ever. *Inc.com, 12/2/2018*

Scanning Documents Has Never Been Easier — Here's How

Apple's iOS 11 app is full of exciting new tricks, but the most useful one is a little buried and definitely a lot less glamorous than most: the document scanner inside the Notes app. You no longer need to use a third-party app to upload your documents; you can do it inside Apple's excellent internal solution.

Just open up Notes, hit the "+" symbol above the keyboard, and tap "Scan Document." Then all you need to do is select your settings, point it at whatever document you're trying to digitize and it'll do the rest. It'll optimize the picture as a scan and make the document as readable as possible. *TheVerge.com, 8/26/2018*