# TECHNOLOGY TODAY

## No Nickel & Dime

Our own CEO, Yuri Aberfeld, was recently featured in Channel Pro Networks online magazine, discussing the most fair and effective ways to structure pricing and service in the Managed Services Provider (MSP) realm. Too often, tricky contract wording, designed to present the 'best price' leads customers into a mountain of extra charges for 'extras'.

IT Support LA features pricing structured to give the client everything they need and more, without skimping on services or piling on additional charges. Yuri notes that our clients never have occasion to feel "nickel and dimed."

To read more, the full article is here: www.channelpronetwork.com/article/simplify-managed-service-sales-customer-pricing.

**July 2018**

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

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

## Do You Safeguard Your Company's Data And Private Customer Information BETTER THAN Equifax, Yahoo And Target Did?

You can't deny that today we are living in an era of unprecedented technological progress. Particularly in the business world, we find ourselves more empowered day by day with the onslaught of fresh applications and features promising to extend our reach and drive success. There's a reason, after all, that business leaders like Virgin Group CEO Richard Branson argue that right now is a better time than ever to start a scrappy new company.

But this trend, in which companies become ever more inseparable from the technologies they depend on, is a double-edged sword.

Though tech continues to break down barriers to success in business, its forward motion is naturally accompanied by a newfound vulnerability. Each development is accompanied by a weakness to exploit – a back door through which hackers can wreak havoc on companies and customers alike.

This should be obvious to anyone who has even the barest awareness of the news. As the list of Fortune 500 companies that fall victim to cyber-attacks grows, we all need to learn from their mistakes and batten down our digital hatches in anticipation of a potential breach.

Last year, the country was shocked to discover that the personal data of more than 146 million people – including driver's licenses, passport numbers, Social Security numbers and a wide swath of other information – had been exposed in an attack on the credit mega-giant Equifax. Hackers infiltrated their systems through a vulnerability in Apache Struts, a tool used to develop web applications, and proceeded to lift a staggering quantity of customer data. The consequences of this attack are still being unpacked even now, but it's safe to say that even beyond Equifax's plummeting stock prices and their trip to PR hell, they've put themselves and the people they serve in a horribly uncomfortable position.

*Continued on pg.2*

*Continued from pg.1*

And make no mistake, the Equifax attack was far from inevitable. You would think that a company sitting on an international treasure trove packed with data from more than 800 million customers and 88 million businesses worldwide would take pains to be responsible digital stewards. But last September, under intensive government and journalistic scrutiny, company officials confirmed that, basically, this enormous breach had all come down to Equifax's failure to adequately patch their Apache Struts platform. You see, there was a known, publicly disclosed bug in the Apache Struts system the previous March. Despite the Apache Software Foundation's subsequent release of a patch eliminating the vulnerability, Equifax didn't install it in time to prevent issues, giving hackers months to easily exploit their systems and gain a foothold.

While the Equifax attack is certainly one of the most high-profile widespread data breaches in history, it's definitely not the only one to affect millions of customers. Yahoo admitted in 2016 that a data breach way back in 2013 had exposed around 1 billion of their usernames, e-mail addresses and passcodes. When Verizon acquired the company last year, they admitted that, upon further review, it looked more like 3 billion accounts had been affected. Also in 2013, hackers infiltrated Target's point-of-sale systems to steal 40 million debit and credit card accounts, thanks to a vulnerability in an

**"Though tech continues to break down barriers to success in business, its forward motion is naturally accompanied by a newfound vulnerability."**


HVAC company they'd hired called Fazio Mechanical Services.

Attacks like these – and the millions of similar ones aimed at small, midsize and massive companies every year – are almost always circuitous and confusing to the average business owner, but they're also preventable. Problem is, especially when it comes to SMBs, most business professionals and their understaffed, underfunded, inexperienced or even nonexistent IT departments aren't equipped to protect their precious data when the hackers come knocking.

Statistics show that, eventually, hackers are going to come for your business – it's all but guaranteed. And if they break through and bring your company to its knees, you probably won't be the next Equifax or Target all over the news with egg on your face. No, your business will probably just fold in on itself with nary a whimper, with everything you've worked so hard to build quietly buckling before your eyes.

Don't let it happen. Address cyber-attacks before they become an issue, and get a talented, experienced, around-the-clock team to defend your livelihood. It takes vigilance, research and constant upkeep to keep the wolves at bay. Protect your business or, before you know it, there won't be anything left to protect at all.

# Help Us Out And We'll Give You A Brand-New Kindle Fire For Your Trouble

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of July.

Simply refer any company with 10 or more computers to our office to receive a FREE computer network assessment (a $397 value). If your referral becomes a new client, we'll rush YOU a free Kindle Fire of your choice as a thank-you (or donate $100 to your favorite charity ... your choice!).

**Simply call us at 818-797-5300 or e-mail us at info@itsupportla.com with your referral's name and contact information today!**

# RDP is BFD

Microsoft's Remote Desktop Protocol (RDP) is the Big Freaking Deal when it comes to your network's weakest entry point for cybercriminals. Used in conjunction with Microsoft's Credential Protocol (CredSSP), it has been identified as the #1 pathway that allows Ransomware hackers to breach networks. It's a two-prong approach: First, the theft of credentials, and Second, the use those credentials to breach the system. That's when you get locked out and the ransom demands begin.

RDP is already built-in to most versions of Windows, and once those computers are connected to the internet, you are vulnerable, and the crooks are waiting. Lists of companies that use RDP are sold on the Dark Web to save the end-point cyber crooks a step. Remember, this is not vandalism, but a very serious and highly profitable business model.

What can you do about it? With so many remote workers in business today, you can't simply remove RDP. As each degree of remote access is different, it's important to have your IT provider structure the access behind your secure VPN. After that, a number of solutions are available, depending on your individual requirements and practices.

Take us up on our offer of a 100% FREE, no strings Cyber Security audit. It is rare that we do not find multiple areas where your network is vulnerable. Call us at 818-797-5300 or visit us at: www.itsupportla.com/free-data-security-analysis/ to arrange your free confidential assessment.

# The Source Of Knowledge Is Experience

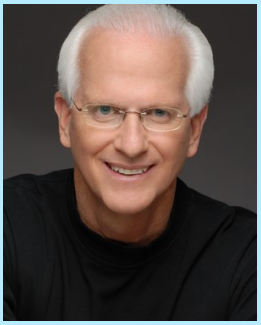
According to the Small Business Administration, entrepreneurs start 543,000 new businesses each month, but only 18% of them ever succeed. Instead, 46% succumb to incompetence, 30% to lack of managerial experience, 11% to lack of experience in goods or services and 13% to other issues, like neglect, fraud or disaster.

You may notice that three of four of these failure triggers relate to lack of experience. That should be no surprise; after all, there's no substitute for raw experience. Even Albert Einstein agreed when he said, "The only source of knowledge is experience."

So, I thought it might be useful to put together a list of business axioms to help you shorten the learning curve and get acquainted with the lessons of experience in bite-size form. These are tidbits I've gleaned across years in the business world, pithy ideas that you should examine closely to see if you're utilizing them in your own approach. Here they are, in no particular order:

- Listen carefully to your clients; they will tell you how to stay in business.
- Minimize company policy and procedures. Simplify every chance you get.
- Under-commit and over-deliver.
- Take time to chat with employees; they too, have good ideas.
- Remember, anyone can be replaced...you included.
- Employee turnover is much more expensive than paying well to begin with.
- Celebrate what your employees do for you.
- A chain is no stronger than its weakest link, so fix or replace it.
- Leaders give more to their staff than just a paycheck.
- If you're going to lose, lose early.
- The person who asks the questions controls the conversation.
- Great leaders take joy in the successes of those under them.
- Praise loudly and blame softly.
- Always push yourself to make continual improvement.
- Don't burn bridges. You'll probably need them again someday.
- Arrogance kills success. Don't let your own arrogance blind you.
- When you go the extra mile, people take note.
- You're not as unique as you may think you are.
- There are many ways to do something; embrace ideas from all generations.
- You can never achieve greatness without a little discomfort in the process.
- You will not learn anything while you are talking. Listen closely and talk less.
- Look sharp. Dressing well helps you exude self-confidence without saying a word.
- Never waste your energy looking for an excuse. Save that energy to look for a solution.
- Smart people learn from their mistakes; wise people learn from other people's mistakes.

I know that's a lot to digest, but comb through these carefully — I guarantee you'll find something useful. One of my favorite quotes comes from Will Rogers: "Good judgment comes from experience, and a lot of that comes from bad judgment." Experience is a cruel teacher. It gives a test before presenting the lesson. That isn't fair, but it's reality. Hopefully you can gain something from the axioms listed above, so your teacher won't be so cruel. Remember, wise people learn from the mistakes of others.



*Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys and 52 Essential Habits For Success, he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

### DON'T Use Public WiFi Until You Read This

If there's one mortal cyber security sin of which we're all guilty, it's connecting to free public WiFi. Whether it's at the coffee shop, hotel or airport, the temptation to check e-mail and surf the web is just too strong to resist. But BEFORE you connect to any free, public WiFi, you need to ensure the connection is legitimate.

It's not uncommon for hackers to set up fake clones of public WiFi access points to try and get you to connect to their WiFi instead of the legitimate, safe public one made available to you. Before connecting, check with an employee of the store or location to verify the name of the network they are providing. And never access financial, medical or other sensitive data while on public WiFi. Avoid shopping online or entering your credit card information unless you're absolutely certain that the connection point you're logged on to is safe and secure.

### How To Use CRM To Create Positive Customer Experiences

Every business in the world lives or dies by its customers. Luckily, customer relationship management (CRM) software has made it easier than ever to facilitate powerful customer interactions and turn even the most skeptical prospects into loyal brand advocates.

First and foremost, CRM empowers businesses to step up their customer service game. Most CRM software includes the ability for customers to create support tickets and submit questions to your team, making it easy to track whether or not their query has been answered and allowing direct chat to resolve issues in a timely manner.

You can also use CRM to segment your customer data. After a customer has expressed interest in your business through website visits or signing up for a mailing list, data will be entered into the CRM data bank, which enables you to track all interactions with that customer and quantify their engagement with your business. This way, you can separate customers into targeted groups to maximize conversions.

*SmallBizTechnology.com, February 16, 2018*

### Knowing These 6 Tricks Will Help You Avoid Phishing Attacks On Your Business

1. No matter what the situation, don't panic or click any links until you know they're legitimate. If you suddenly receive an odd e-mail from a coworker, you're right to be suspicious. Investigate before clicking anything.
2. Keep an eye out for red flags. Hackers will often masquerade as a legitimate party, but many times there will be something off about their e-mail addresses or information.
3. Notify the company that's being impersonated. Find the company that the hackers are pretending to be, contact them and let them know the situation. Also click on the arrow next to Gmail's reply button and click "report phishing."
4. Share the phishing trick on your social media channels.
5. Alert your friends and family about the attack.
6. Let your business know that phishers are trying to penetrate your network.

*SmallBizTrends.com, February 5, 2018*