

TECHNOLOGY TODAY

Inhospitability

Maybe it was a lovely vacation or a productive business trip, until you discover your personal information, including your payment cards, has been stolen in a gigantic Data Breach following your stay at any of the Marriott International's Starwood properties on or before September 10, 2018. These hotels & resorts include W Hotels, St. Regis, Sheraton, Westin, or Le Méridien Hotels & Resorts, and other locations. You're not alone: you are one of over 500 million other customers.

Once you take personal or corporate information on the road, you are entrusting that data to your host. If you have visited one of these hotels, we strongly advise you to identify any and all persons and payment cards that have been exposed at these locations. Do it quickly, as your information is already up for sale.

For this and any other occasions where you suspect your credit information has been compromised, take the necessary steps to protect yourself. To find out what you need to do, please visit us at:

www.itsupportla.com/breach-assistance/

January 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.



The Top 3 Things I Learned From Shark Tank's Robert Herjavec For Growing A Business From Scratch To Multimillion-Dollars

Robert Herjavec was born poor in former Yugoslavia in the midst of a widespread communist reform that left little room for dissidents. He might have stayed there forever except for the fact that his father was one of these dissidents – and a vocal one at that. So much so, in fact, that he was thrown into jail 22 times for speaking out against the government. After the final time, Herjavec's father gathered his things, his children and his wife and crossed the border into Italy. From there, he got on a boat and, like millions of immigrants just like him, made his way across the Atlantic Ocean to Canada.

But that's not what Robert Herjavec, one of the famous investors on ABC's *Shark Tank*, is known for. He's more known for building companies out of nothing, including the massive IT

security firm Herjavec Group, and turning them into multimillion-dollar successes. Watching him from the audience at a recent conference event, I was struck not only by his eagerness to share all he's learned in the industry, but by his humility. I suppose when you're the living embodiment of a rags-to-riches story, you gain an appreciation for exactly what it takes to realize your vision for a successful business.

Herjavec had a lot to say during his talk, but there were three points in particular that stood out for me.

1. IT ALL COMES DOWN TO SALES.

The one thing that Herjavec really wanted to hammer home with each and every one of us is the importance of sales. "Nothing happens until you sell something," he told us. "What's the

Continued on pg.2

Continued from pg.1

difference between really big companies that grow and really small companies that stay the same size? Sales."

Over the years, Herjavec has bought and sold 13 companies, and he's learned the best approach to suss out whether a potential buy is worth it or not. One of the questions he always asks is, "How do you guys get customers? How do you guys find new business? And if the answer is anything along the lines of 'word of mouth,' I know these guys aren't going anywhere." The fact is that word of mouth is hard to control and almost impossible to scale. To truly drive the growth of your company, he says, you can't think of sales as "a foreign object that controls what you do." You have to see it for what it is - "an extension of what you do."

2. NO, REALLY - IT ALL COMES DOWN TO SALES EVERY DAY.

"Nobody in this room makes money for shuffling paper," Herjavec said. "If one of your top three tasks every day isn't 'Sell something,' you're going to fail." The only way to create "constant forward momentum" is by bringing in new revenue, and the only way to do that is to sell.

3. YOU CAN'T BE AFRAID TO SELL.

We all know that people in any industry are always

"The minuscule amount you'll save by hiring a cheap support company will be vastly outweighed by the long-term cost of your decision."



worried about overloading themselves. "We're struggling to serve the customers we have already," they say. "What happens if we really do bring in a bunch of new ones?"

This line of thinking will get you nowhere. "It's a common fallacy," Herjavec said. "Engineers want to make it perfect before they sell it. True entrepreneurs jump out of the airplane and have the confidence that they'll figure out the parachute on the way to the bottom."

The key is to find your niche. Sales takes a long time to learn - years and years of trial and error. But if you can "figure out who you're selling to," as he put it, you're already far ahead of your competition. Find the factor that differentiates you from the sea of similar companies, leverage your strengths and sell until you drop. That's the path to success and, as hard as it is, there isn't any other. Go on *Shark Tank* sometime and Robert Herjavec will be the first to tell you.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"



Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain, nontechnical English 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.itsupportla.com/protect/
or call our office at (818) 797-5300

Anticipation!

It's not a matter of IF, but of WHEN!

So you've got your firewall and Anti-Virus in place, thinking they will protect you from Ransomware and Data Breaches, and they will defeat the easiest threats, but remember: the bad guys never sleep. They know what you've got, and in the big business of cybercrime, they spend tons of money on R & D, finding the quickest way past or around the newest defenses.

Instead of sitting back in your network castle waiting for the inevitable attack, with the false sense that your moat and your walls will keep the invaders out, you and your IT provider must anticipate the attack. Sure, everyone thinks they're proactive, but are you?

If your IT provider does not have an active MDR (Managed Detection & Response) protocol in place, then you are just waiting for the ENEMY to show you where your defenses are weakest, and that is an expensive lesson.

An MDR protocol consists not only of your IT provider, whether in-house or outsourced, engaging in full-time threat hunting, but in joining forces with your own employees. The biggest threat remains the errant or ignorant click of the mouse by untrained users. The collaboration between IT provider and your office staff is an absolute 'Must Have'. If none of your users ever opened an email or went on the internet, this symbiotic relationship would be unnecessary, but like it or not, we're all in this fight together.

Those days are long gone when it was as simple as 'The computer's broken – call the guy', and if you are still operating that way, then you are opening yourself up to catastrophe. In order to do business you have to be connected to the world, and in turn, the world, including the scammers, phishers, extortionists and thieves are connected to you. For that, you either pay a price in ransom or in vigilance.

Take us up on our offer of a FREE Cyber-Security assessment and see where you stand. See if you're as safe as you think you are: most are not, by a horrifying margin. Contact us at 818-797-5300 or at: www.itsupportla.com/free-stuff/free-network-security-assessment/

The Most Effective Closing Technique



Of all the things I've done during my entrepreneurial career, selling has been the one constant. Ever since my first job out of college, I had to sell to make a salary. When starting my first business, I had to sell to survive. Even the first book I wrote would have been nothing without a huge selling effort. As a result, I've become a lifelong fan and student of great selling techniques.

My favorite technique used to be the 1-to-10 close. You know, where you ask your customer, "On a scale from 1 to 10, where do you stand on proceeding with us?" And then when they answer, you ask what you can do to make it a 10. The strategy even worked occasionally, despite the fact that it was exactly what I should *not* have been doing.

People resist suggestions. If you're a smoker and I say, "You need to stop smoking – it's bad for you," you'll roll your eyes and say, "Yeah, I know." Then you'll light up a smoke and blow it in my face. We automatically do the opposite of what people suggest.

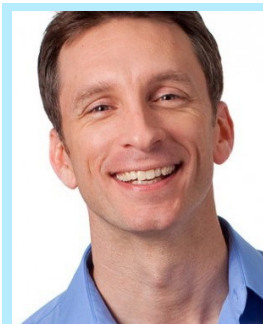
Later in my career, I stumbled across another 1-to-10 technique, which is still the most effective closing method I've ever experienced. When asking people where they stand on the scale, no matter what they say, I say something like, "I

didn't expect you to pick a number so high! From our discussion and your body language, I actually thought you were much lower. Why did you pick a number that high?"

When I suggest a number lower than what they say, people naturally resist my remark and want to go higher. Now they argue about why the number they picked – say five – is not that high, and maybe even change their number to a six or a seven. But no matter what, they're arguing in their own head over why they should go with you.

Tom Sawyer knew this technique. When he acted up and was forced to paint a fence as punishment, his buddies started teasing and ridiculing him. But he just kept painting and said, "Not just anyone can paint a fence." By the time he convinced them that they weren't capable of painting a fence, they began begging him to let them have a try. Only then did he let them, while he relaxed in the shade.

It's a simple strategy, but it works. You can persuade your customers all day to work with you and they won't bite – but get them to convince themselves, and you're in business.



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 Provenius Group. He is also 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.

■ 5 Sneaky Tricks Cybercriminals Use To Hack Your Network

1. PHISHING. Woe to you and your business if you haven't heard of this one yet. By using an email, chat, web ad or website impersonating a legitimate organization, hackers get members of your team to click and install malware.

2. BAITING. Baiting uses an enticing item to lure employees into giving up personal data, such as a music or movie download or a mysterious flash drive left around the office.

3. QUID PRO QUO. It's like baiting, except that hackers offer a service instead of an item in return for private data.

4. PRETEXTING. This is a type of phishing in which a hacker poses as a respected colleague or member of your organization in order to boost private data.

5. TAILGATING. It occurs when an unauthorized person physically follows your employees into restricted areas.

SmallBizTrends.com, 9/20/2018

■ Don't Wait 191 Days To Realize There's Been A Data Breach — By Then, It's Too Late

According to a 2017 report by research firm Ponemon, it takes an average of 191 days for a company to realize it's been compromised by a data breach. This number should scare anyone. The longer you take to recognize and respond to a breach, the more criminals can steal and the bigger the damage becomes. What's more, your delayed reaction will leave you fewer options to mitigate the disaster. To survive, you need to stay on top of your cyber security with a team of dedicated professionals keeping tabs on attacks, strengthening your barriers and responding within hours, not days, if the worst ever happens.

SmallBizTrends.com, 10/30/2018

■ Top Employee Retention Strategies To Keep Your Workers Motivated And Productive

Successful business owners do more than focus on the bottom line. They work to make their office a genuinely enjoyable place to work, creating an environment that fosters loyalty and success in their team over time.

Keeping top performers from jumping ship should obviously be your priority, but these are often some of the most difficult people to keep on board. As they shoulder extra responsibilities and bend over backward to serve your company, they may start to feel undervalued. It's your job as manager to actively seek out any pain points they may be experiencing and resolve them. Regular employee surveys and open lines of communication between teams and management can curb problems before they turn happy workers into disgruntled sandbags.

Of course, no matter how easy you make it for them to do their job, they're going to leave if you still can't give them what they're worth. In a recent Glassdoor survey, it was revealed that over 45 percent of people quit their job because they've been offered more money elsewhere. CEOs tend to be fond of making excuses for avoiding raises and robust benefits, but employees know what they're worth, and they know what they need to stick around.

HomeBusinessMag.com, 10/12/2018

