

# CYBERSECURITY CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

## TECH TIP OF THE MONTH

Free VPNs (Virtual Private Networks) seem like a great way to save a few bucks, but they can be dangerous.

Free VPN services are typically not very secure. Since the software company isn't collecting a fee from you to pay employees to keep up with updating the software, it often doesn't provide adequate protection.

Some of these free versions can also contain malware. Scammers can set these up, trying to take advantage of business owners looking to cut costs.

They can also collect and sell your private data, which is how they keep up with any updates.

The best thing to do is just not risk it and opt for a paid version. We can help you choose the right one for your business.



## WHAT DO YOU DO WHEN A COMPANY COMPROMISES YOUR DATA?

With the rise in cyber-attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, SSNs, etc. – the most commonly breached type of data. A recent

example is ChangeHealthcare, breached in February of this year. Due to the breach, it's estimated that one-third of Americans – possibly including you – had sensitive information leaked onto the dark web.

So now what? What do you do when you receive a letter in the mail from your health care provider or favorite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals. When sensitive information leaks, you'll have to do some recon to protect your

*continued on page 2...*

*This monthly publication is provided courtesy of Heath Couchman, CEO of Advent Technologies.*



### OUR MISSION:

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

...continued from cover

accounts from suspicious activity. Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

## What To Do After Your Data's Been Leaked

### 1. First, make sure the breach is legit.

One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

### 2. Figure out what data was stolen.

After speaking directly with the company, determine what data was stolen. Credit cards can be easily replaced; Social Security numbers, not so much. You'll want to know what was

compromised so you can take the necessary steps to monitor or update that information.

### 3. Change passwords and turn on MFA.

After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

### 4. Monitor your accounts.

Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorize. They may be a sign of identity theft. If your credit card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

### 5. Report it.

If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like

local law enforcement or the Federal Trade Commission. They can provide guidance and next steps on how to protect your identity.

### 6. Be aware of phishing attempts.

Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even more sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

### 7. Consider identity theft and data breach protection.

Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your SSN. It's a time-consuming process to replace a Social Security card. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimize a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

## The Northern California Business Owner's Guide To IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Small Business (And How To Get Exactly What You Need Without Unnecessary Extras, Hidden Fees And Bloated Contracts)

### Read This Guide and You'll Discover:

- The 3 most common ways IT services 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 added costs later on that you didn't anticipate.
- 21 revealing questions to ask your IT support firm BEFORE giving them access to your computer network, e-mail and data.



Download your FREE copy today at  
[www.adventtechnologies.net/itbuyersguide](http://www.adventtechnologies.net/itbuyersguide)  
 or call our office at (916) 476-2992.



# MICHAEL MICHALOWICZ

EXPLAINS HOW TO  
BUILD A TEAM THAT CARES  
ABOUT YOUR COMPANY'S  
SUCCESS AS MUCH AS  
YOU DO



Early in his career, Mike Michalowicz was eager to announce to his team a new corporate vision for the year: a \$10 million revenue goal. However, what he imagined would be one of his greatest visionary moments as a leader was one of his biggest mistakes.

After revealing the vision to his team, “it was total silence,” Michalowicz explained to a room of business leaders at a recent industry conference. “A colleague came over to me and said, ‘Mike, if we achieve \$10 million in revenue, you get the bigger house. You get the new car. That’s your vision. What about our vision?’” This was a transformative learning moment for Michalowicz, who committed himself to learning what it takes to be a GREAT leader.

Today, Michalowicz is the author of several books, including *Profit First, Get Different, The Pumpkin Plan* and other small business must-reads. He’s an entrepreneur and speaker teaching other leaders how to build and retain unstoppable teams who care about the company’s success as much as you do, so you’ll be happier, grow faster and create an environment where everyone flourishes.

## How To Build An Unstoppable Team

### 1. Most leaders tell their team what to do.

Great leaders ask their team what they could do. One of the Baltimore Museum of Art’s most successful exhibits was curated by 17 museum guards. The idea came from a conversation between a curator and a guard around what the guard did day-to-day. He revealed how much he learned about the art from patrons and what interested them. Museum leaders quickly learned this wasn’t unique to the one guard, and a group was assembled to create “Guarding the Art.” Michalowicz explains that great leaders encourage ownership by asking, “What could we do?” rather than always telling their employees what to do.

### 2. Great leadership assembles and unifies.

The movie *The Boys in the Boat* recounts how an inexperienced US rowing team won gold in the 1936 Olympics. The leader helped the team connect, communicate and work together to win against all odds. He fostered deep trust within the team, which Michalowicz says distinguishes great leadership in any circumstance.

### 3. Great leaders follow a FASO model.

Michalowicz’s research and experience in leadership culminate in a four-part model he calls “FASO.” Leaders who want to be great can use FASO to assemble an unstoppable team.

- **F – “Fit.”** When hiring a new team member, they must be an ideal fit for the organization, and the organization must be an ideal fit for them.
- **A – “Ability.”** Great leaders look for people’s raw potential. Do they have curiosity, desire and a thirst for the role? That’s what great leaders hire and recruit for, not simply experience and innate ability.
- **S – “Safety.”** Great leaders account for their team’s physical, relational and financial safety. They ensure that people feel safe in how they are treated and where they work, they have a transparent financial culture and they educate their team on personal finances.
- **O – “Ownership.”** “When we’re forced to comply, we’ll seek to defy,” Michalowicz says. Great leaders encourage their team to personalize, gain intimate knowledge of and control aspects of their work.

Above all, Michalowicz says, “No one cares how you care; they care THAT you care.” Show your team you care by working to incorporate these great leadership approaches in your organization.

## SHINY NEW GADGET OF THE MONTH

### Targus Coastline EcoSmart Backpack

With its thoughtfully engineered and comfortable design, the Targus Coastline EcoSmart Backpack is an excellent choice for professionals on the move. Its standout feature is the SafePort® Sling Protection System, which ensures that laptops up to 16” are securely cradled against the bumps and knocks of a daily commute.



Additional padded straps, front pockets and a 22L capacity leave plenty of room for everything you need on a long commute or a day away from the office. Equally impressive is the backpack’s commitment to environmental responsibility. Made from 69% certified Ocean-Bound Plastic, the backpack is durable and resistant to wear and tear but also contributes to reducing plastic waste in our oceans and empowering coastal communities.

## CARTOON OF THE MONTH



“Here’s what you’re going to do. You’re going to give those 3 million people their credit card numbers back and you’re going to say you’re sorry.”



## DON'T MAKE THIS MISTAKE WITH YOUR HOME'S SMART TECH

Smart devices are so pervasive throughout our homes that it's hard to imagine what life was like before them. From door cams that show us when our kids get home to AI-powered devices that keep track of grocery lists and play our favorite music while we cook, we truly live in "smart" homes.

But unlike devices of the past, you can't "set and forget" smart devices. These tools are connected to the Internet, where hackers keep a close eye out for unprotected devices. When they find a device with a weak password, they can access it and carry out terrifying crimes like watching your family through a home camera. Before you plug in your smart device, follow these simple steps to make sure it's not an open door for peering eyes.

### Pros And Cons Of Smart Devices

When hackers find an unprotected device – like an indoor cam that you never bothered to change the default password to – they can access sensitive information on your account, including your address, birth date, e-mail address and phone number. Criminals use this information to create a profile about you and carry out targeted attacks. A family in Mississippi even had a hacker taunt their young daughter through their Ring camera.

Thankfully, you can take a few simple security steps to avoid becoming a victim of your smart device.

### Steps To Keep Your Smart Home Safe

- 1. Change the default login information immediately.** Default passwords are low-hanging fruit for hackers, so be sure to change this to a new, stronger password right away.
- 2. Make sure your WiFi is secure.** If your WiFi password is a few years old or you use the same password on other accounts, change it to a stronger password.



**3. Enable multifactor authentication (MFA) in security settings.** This way, users can only log in with a security code or authenticator app, making it nearly impossible for hackers to get in.

**4. Regularly update the device.** Updates fix issues or add new features that may improve your security. Don't skip these updates. If your smart device doesn't update automatically, set a reminder in your phone to check for updates periodically.

**5. Consider separate networks.** Many WiFi providers offer guest networks. Consider connecting smart devices to a home guest network separate from the one that your phones or laptops are on. This way, if a smart device is hacked, it's not a straight shot to devices holding more valuable information.

The biggest mistake smart-device users make is thinking they can plug in their devices and walk away. These tips go a long way toward ensuring that your device isn't an open door to creepy criminals.

## INSIDE THIS ISSUE

What Do You Do When  
A Company Compromises  
Your Data? P. 1

What You Should Expect To  
Pay For IT Support For Your  
Small Business  
P. 2

Mike Michalowicz Explains  
How To Build A Team That  
Cares About Your Company's  
Success As Much As You Do  
P. 3

## THE GEEK WAY:

The Radical Mindset That  
Drives Extraordinary Results

By Andrew McAfee

When we have a big problem, we like to go to experts who don't just like what they do but are downright geeky about it. Geeks are known for being intelligent and efficient problem-solvers, but what if we could all benefit from a geeky mindset to perform better in our work and lives?



In *The Geek Way: The Radical Mindset That Drives Extraordinary Results*, Andrew McAfee explores four "norms" – science, ownership, speed and openness – that define geek culture. He explains that when these norms are aligned, it taps into our human superpowers: our ability to cooperate intensely and learn quickly. This book blends science, history and real-world examples to provide insights into harnessing geek culture for innovation. *The Geek Way* is a compelling read for anyone interested in channeling their inner geek to improve their ideas, business or community.

## ARE YOU USING THIS HELPFUL GOOGLE CALENDAR HACK?

It's a bit embarrassing when you log in to your computer at 9:00 a.m. only to realize you missed the all-team Zoom meeting at 8:30 a.m. Thankfully, Google Calendar offers a helpful hack: daily agendas. With this feature, you can send yourself a daily agenda first thing in the morning so you know everything planned for the day. To set it up, log into your Google account and go to

Settings. Find "Settings for my calendars" > "Other notifications" > "Daily agenda." The default is set to "None," so click on it and change it to "Email." Now you have a daily agenda automatically sent to your inbox before you even get out of bed!

