

modern business **IT.advisor**

"Insider Tips To Make Your Small Business Run Faster. Easier, and More Profitably"

Bay Area's Award-Winning IT & Cybersecurity



TruAdvantage Recognized for
Excellence in Managed IT Services

OCTOBER 2025



Kayvan Yazdi,
CEO of
TruAdvantage

OUR MISSION:

To become a trusted partner to our clients and impact their success by delivering technology, education, and process.

THE TRUTH ABOUT CYBERSECURITY

EVERY BUSINESS LEADER SHOULD KNOW

There are many common myths when it comes to cybersecurity, and, unlike harmless stories, these myths can leave you with gaping holes in your company's cybersecurity defenses. Here are five common myths and the truth behind them.

Myth No. 1: It Won't Happen To Us.

There's a common belief among small and medium-size businesses that they are too small to be a target for attackers. But this isn't the case; in fact, some cybercriminals target SMBs specifically, with the knowledge that SMBs are less likely to have the resources for reliable cybersecurity.

Cyberattacks happen to organizations of all sizes, in all verticals and geographies, and hit 80% of businesses. The global financial toll? A projected \$9.5 trillion. And while large

corporations can take the hit and recover, a single ransomware attack has the potential to put an SMB out of business.

So, regardless of what type of business or organization you have, you must protect yourself from cyberattacks and reduce your exposure. Always assume you are a target — because you are one.

Myth No. 2: If It Worked Then, It'll Work Now.

It's very common for decision-makers to reason that since they've never been breached in the past, they won't be breached in the future, either. However, that belief doesn't account for the rapid pace at which technology — and cybercrime — are evolving.

Continued on Page 2 ...

... continued from Cover

The threat landscape is constantly changing, and there is a very real game of cat-and-mouse at play. If you're not moving forward, you're moving backward. Effective security is a cycle of anticipation, adaptation and action.

Myth No. 3: Once Secure, Always Secure.

Unfortunately, technology is fluid — just like your business. Every time you bring on a new member of staff and add new devices, your technology's configuration shifts. As it does, it creates new avenues of attack from cybercriminals.

That's why continuous monitoring and management are necessary to maintain security integrity. The attack surface stretches beyond common focus areas, so strong cybersecurity demands a holistic, proactive, continuous approach.

Myth No. 4: Business Optimization Is Incompatible With Security.

Many organizations assume that security initiatives create operational friction — delaying releases, adding red tape and increasing costs. This outdated thinking frames security and business optimization as mutually exclusive, as if improving one must compromise the other.



While these perceptions may have roots in the past, they don't reflect modern practices. Today, security enables optimization. That means minimizing both waste and risk — including security risk.

In the end, secure systems are more resilient, predictable and cost-effective. This makes security a driver of business performance, not a barrier.

Myth No. 5: A Strong Password Is All I Need.

Creating a strong password (at least 16 characters long and a blend of letters, numbers and special characters) for each account is important, but it's not the only step needed to keep your data secure.

For one, every account and device needs a *unique* password. If you reuse passwords, it means that if one of your accounts is hacked, all of your other accounts are at risk. To store all your unique passwords, we recommend a password manager!

Enabling MFA for every account will double your protection. The few seconds required to enter a code sent to your phone is well worth the extra security.

That said, there are plenty of other vulnerabilities that savvy hackers can exploit to attack your business's data. That's why working with an MSP is a critical component of maintaining your company's cybersecurity.

FREE REPORT DOWNLOAD

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

You'll learn:

- The three most common ways IT 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



Claim your FREE copy today at truAdvantage.com/itbuyersguide



CARTOON OF THE MONTH



DR. PHIL

PUSHES BUSINESS OWNERS TO 'OWN IT' — IN LIFE AND IN BUSINESS



In a recent interview, Dr. Phil McGraw, celebrity psychologist and talk show host, gave frank advice on what it really means to be in business — and how to stay true to themselves while doing it.

Stay True To Passion And Stand Out.

“I don’t do anything that I’m not a hundred percent passionate about. And I never wanted to be a member of the herd. I didn’t want to be a face in the crowd,” McGraw said. “I wanted to market my education in a way that set me apart from the rest of the industry. I think you have to do that [in business].”

Define And Articulate Your Differentiator.

“You have to know what separates you from everybody else that thinks they do what you do. What do you bring to the table that nobody else does? What do you do that’s different than everybody else? If you don’t know what your differentiator is, if you can’t articulate it and don’t market it in an easily perceptible way, then you aren’t really in business yet.”

You Are Your Own CEO.

“I think every one of us is a company of one,” said McGraw. “I don’t care if you work for the United States post office. Every one of us is a company of one — and you are your own CEO. Then the question becomes: How are you doing in managing your career? How are you doing in managing your stock? How are

you advancing your game? What is the world willing to compensate you for? If you can’t articulate that with clarity and precision, then you’re not really in business yet. You haven’t gotten the courage.”

Define, Commit, And Own Your Brand.

“No one is going to confuse me with anyone else, just like you’re not going to confuse McDonald’s with a great steakhouse [brand]. That’s important to me,” he said. “Define your brand, decide what it is, make a commitment to it, and ride that horse to the finish line. You’ve got to decide what it is that you’re selling and own it. Be who you are on purpose. Don’t just get up and react to the world. Decide who you are and do that on purpose. Don’t apologize for it. Own it.”

Authenticity Is Key To Facing Criticism.

“In the pursuit of that, you will face criticism. Not everyone will like you and your brand. But that’s exactly why you have to believe in what you’re doing passionately,” says McGraw. “You can’t just put it on. You have to believe it. A lot of people don’t like some of the things I do. And I get that. But how boring would this world be if we were all the same? We have a divisive world, in terms of ideas. But you have to believe what you believe. Then when somebody disagrees with you, if you’re authentic in your position, you won’t have a problem standing with it.”

SHINY NEW GADGET OF THE MONTH



BenQ ScreenBar Halo Monitor Light

The BenQ ScreenBar Halo is a sleek USB powered LED monitor light designed with an asymmetric optical system that directs soft, glare free illumination onto your desk while avoiding screen reflection. With adjustable brightness and color temperature, you can dial in the perfect lighting using the wireless controller. It even has a backlight to reduce contrast with your surroundings. Plus, the auto-dimming feature adapts to your room’s lighting, so it’s always just right. No messy cords or mounts — just clean, functional lighting that protects your eyes and keeps your setup looking sharp.

INSIDE THIS ISSUE

The Truth About Cybersecurity Every
Business Leader Should Know ... **1**

Dr. Phil Pushes Business Owners To
'Own It' — In Life And In Business ... **3**

Don't Wait To Upgrade Old Tech ... **4**

5 SIGNS

YOU'RE DUE FOR A TECH UPGRADE



Holding onto old tech may seem budget-friendly, but it can cost you far more in the long run. Outdated systems reduce productivity, increase downtime and pose serious security risks.

The Hidden Costs Of Old Tech

Aging hardware slows your team down. Frequent crashes and sluggish performance affect efficiency, while unexpected failures can halt work altogether. Even worse, outdated software and operating systems often go unpatched, leaving your business vulnerable to cyberattacks. This can result in data breaches and failed compliance audits.

Here's how to know when it's time for an upgrade:

1. You're Still Running Windows 10 Or Older.

Microsoft will stop supporting Windows 10 in October 2025. Without updates, your systems become easy targets for cybercriminals. Plan your upgrade to Windows 11 now to avoid compliance and security issues.

2. You're Constantly Calling IT For The Same Problems.

If your team faces repeated crashes or sluggish systems, your tech is likely on its last legs. Constant IT support drains time and productivity — it's more cost-effective to upgrade.

3. Your Software Isn't Compatible With New Tools.

Legacy systems often don't integrate with modern tools like cloud platforms or mobile apps. This limits your ability to innovate, scale and serve clients efficiently.

4. Your Devices Are Slowing Everyone Down.

Long boot times, frozen screens during meetings or frequent system crashes signal poor performance. Devices older than 3–5 years should be evaluated for replacement, especially if they hinder your workflow or energy efficiency.

5. Your Security Tools Are Outdated.

Firewalls and antivirus programs need regular updates. Outdated defenses can't keep up with evolving threats, making your business an easy target for ransomware.

Final Thoughts

While upgrades may feel expensive upfront, relying on outdated tech can quietly drain your resources. Strategic, affordable upgrade plans are available — and they're essential to keeping your business secure and productive.