



# TECHNOLOGY TIMES

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



## JAY HILL

Many businesses are moving from on-site backups to storing their data only in the cloud. This has become a popular

trend. I personally store things in the cloud. It is effective and efficient. However, storing in the cloud should not replace backing up your server's data on-site. You should back up data stored in the cloud because cloud storage providers aren't immune to data loss. For example, cloud providers are susceptible to outages, hackers, and server crashes, which can cause data loss. Even large cloud application providers recommend backing up data stored in their platforms. I back up everything on-site that I store in the cloud because I know that one of those instances that could cause data loss in the cloud is very probable. We use Datto as our on-site backup because it is reliable, encrypted, and easy to restore. **If you do not have an on-site backup in addition to your cloud storage, please give me a call. Your data needs to be protected.**

*This monthly publication is provided courtesy of Jay Hill, President of Network Providers, Inc.*

## 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.**



## 3 CYBER SECURITY MYTHS THAT WILL HURT YOUR BUSINESS THIS YEAR

Working amid the ever-changing currents of technology and cyber security, businesses often find themselves entangled in a web of misinformation and outdated ideas. But failing to distinguish between myth and fact can put your business's security at serious risk.

Based on expert research in the field, including CompTIA's 2024 global State Of Cybersecurity report, we will debunk three common misconceptions that threaten to derail your success in 2024.

### Myth 1: My Cyber Security Is Good Enough!

**Fact: Modern cyber security is about continuous improvement.**

Respondents to CompTIA's survey indicated that one of the most significant challenges to cyber security initiatives

today is the belief that "current security is good enough" (39%).

One of the reasons businesses may be misled by the state of their security is the inherent complexity of cyber security. In particular, it's incredibly challenging to track and measure security effectiveness and stay current on trends. Thus, an incomplete understanding of security leads executives to think all is well.

Over 40% of executives express complete satisfaction with their organization's cyber security, according to CompTIA's report. In contrast, only 25% of IT staff and 21% of business staff are satisfied. This could also be accounted for by executives often aving more tech freedom for added convenience while frontline staff deal with less visible cyber security details.

*continued on page 2...*

...continued from cover

“Either way, the gap in satisfaction points to a need for improved communication on the topic,” CompTIA writes.

Get your IT and business teams together and figure out what risks you face right now and what needs to change. Because cyber security is constantly changing, your security should never be stagnant. “Good enough” is never good enough for your business; vigilance and a continuous improvement mindset are the only ways to approach cyber security.

## Myth 2: Cyber Security = Keeping Threats Out

**Fact: Cyber security protects against threats both inside and outside your organization.**

One of the most publicized breaches of the last decade was when BBC reported that a Heathrow Airport employee lost a USB stick with sensitive data on it. Although the stick was recovered with no harm done, it still cost Heathrow £120,000 (US\$150,000) in fines.

Yes, cyber security is about protection. However, protection extends to both external and internal threats such as employee error.

Because security threats are diverse and wide-ranging, there are risks that have little to do

with your IT team. For example, how do your employees use social media? “In an era of social engineering, there must be precise guidelines around the content being shared since it could eventually lead to a breach,” CompTIA states. Attacks are increasingly focused on human social engineering, like phishing, and criminals bank on your staff making mistakes.

Additionally, managing relationships with third-party vendors and partners often involves some form of data sharing. “The chain of operations is only as strong as its weakest link,” CompTIA points out. “When that chain involves outside parties, finding the weakest link requires detailed planning.”

Everyone in your organization is responsible for being vigilant and aware of security best practices and safety as it relates to their jobs. Make sure your cyber security strategy puts equal emphasis on internal threats as much as external ones.

## Myth 3: IT Handles My Cyber Security

**Fact: Cyber security is not solely the responsibility of the IT department.**

While IT professionals are crucial in implementing security measures comprehensive cyber security involves a multidisciplinary approach. It encompasses not only technical aspects but also policy, development, employee training, risk management and a deep

understanding of the organization’s unique security landscape.

Because each department within your organization involves unique risks, people from various roles must be included in security conversations. But many companies are not doing this. CompTIA’s report shows that while 40% of respondents say that technical staff is leading those conversations, only 36% indicate that the CEO is participating, and just 25% say that business staff is involved.

“More companies should consider including a wide range of business professionals, from executives to mid-level management to staff positions, in risk management discussions,” CompTIA writes. “These individuals are becoming more involved in technology decisions for their departments, and without a proper view into the associated risks, their decisions may have harmful consequences.”

Business leaders and employees at all levels must actively engage in cyber security efforts, as they are all potential gatekeepers against evolving threats.

## Don’t Listen To Myths

By embracing a mindset of continuous improvement, recognizing the wide range of threats and understanding the collective responsibility of cyber security, your business will remain safe, resilient and thriving, no matter what the future holds.

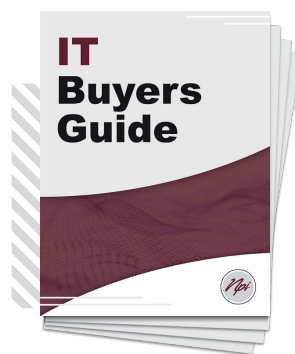
## FREE REPORT DOWNLOAD:

### The Business Owner’s Guide To IT Support Services And Fees

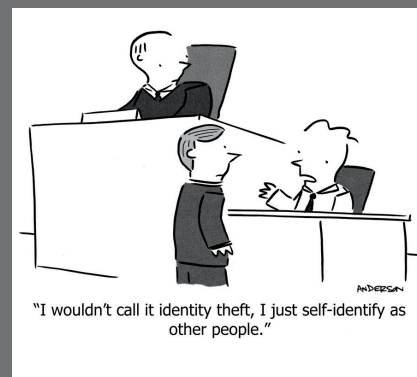
#### You’ll Learn:

- 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 [NetworkProvidersInc.com/itbuyersguide](https://NetworkProvidersInc.com/itbuyersguide)**



## CARTOON OF THE MONTH



## RETIRED NAVY SEAL SHARES THE KEY TO BUILDING AND LEADING A HIGH-PERFORMANCE TEAM



Most business leaders strive for one thing: to be a strong and competent leader of a high-performing team. To do this, they'll try just about anything, from free lunches to daylong team-building retreats. Although these are helpful, high-performing teams don't begin with external motivators. They begin when leaders embrace a culture of extreme ownership.

"Extreme ownership is pretty straightforward," Jocko Willink says. "You're not going to make any excuses. You're not going to blame anybody else. When something goes wrong, you're going to take ownership of those problems and get them solved."

Willink is the author of the New York Times bestseller *Extreme Ownership: How U.S. Navy SEALs Lead And Win*. He explains that the same leadership concepts that enable SEAL teams to succeed in the most intense circumstances can also help businesses win again and again.

As a young SEAL, Willink noticed that a culture of finger-pointing grew when blame was directed toward a person or a team. When that happens, "no one solves the problem," he says. However, when leaders owned issues and responsibility for finding a solution, the team reflected that ownership. "It actually made the other people inside the platoon have the same attitude. They'd say, 'It was my fault; let me fix it,'" Willink explains.

Eventually, Willink went on to fill leadership roles within the SEALs, learning to embrace personal accountability and team empowerment. Now a retired SEAL officer and co-founder of the leadership consulting firm Echelon, he's worked with hundreds of civilian companies on extreme ownership, finding the

same results: when leaders take ownership of problems, the entire team is more likely to be high-performing and successful.

### How To Create An Extreme Ownership Culture

"The biggest thing you've got to overcome is your ego," Willink explains. Pointing out that someone didn't do their job right or that the marketing plan wasn't carried out correctly doesn't solve the problem. "You're the boss. You own it," Willink says. When one person takes ownership, it spreads. "That's what develops the culture."

Although extreme ownership starts with the boss, the key to a high-performing team is to empower individuals to take responsibility for projects and tasks too.

"If you want people to take ownership, you have to give them ownership," Willink says. This way, you empower your team to make decisions while you serve as a reliable guide and offer direction when needed. "Put them in positions where they make decisions, make mistakes and learn to be honest with you," he says. If you're not getting the behaviors you need, you can study it and start to correct it by figuring out what support you can provide.

Willink points out that there will always be team members who don't embrace ownership. But when extreme ownership is a culture, they'll naturally get weeded out.

Those who are ready to step up, however, will rise to the top. "There's something more important to many people than how much money they make," he says. "That is control over their destiny, autonomy and freedom."

### SHINY NEW GADGET OF THE MONTH

#### JSAUX USB Data Blocker



Last year, the FBI warned consumers not to use public charging stations because hackers were installing malware into USB ports and stealing data. If you forget your charger, the JSAUX USB-A Data Blocker is a game-changer for secure charging when you're on the go.

Designed exclusively for charging with no data-sync function, it's perfect for public charging stations in airports, hotel lobbies and coffee shops, eliminating hacking risks. It offers a rapid 2.4A charge and works with a wide range of devices. Compact, portable and cheap, the USB Data Blocker is the no-brainer companion you need in your travel backpack right now!

FIND US  
@NetworkProvidersInc  
on Facebook, Instagram  
and LinkedIn

Even if you're a  
small company,  
if you have ANY  
sensitive data...

You Are A  
Target For  
Cybercriminals.





## OUR SERVICES

- Cybersecurity
- Managed & Co-Managed IT
- Compliance

## CONTACT US

NPI Sales  
385.463.3366

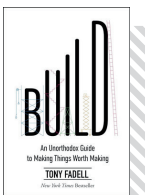
NPI Website  
NetworkProvidersInc.com

PRSRT STD  
U.S. POSTAGE  
PAID  
AMERICAN FORK, UT  
PERMIT NO. 51

## BUILD: AN UNORTHODOX GUIDE TO MAKING THINGS WORTH MAKING

By Tony Fadell

*Build* is an indispensable read for any business owner looking for motivation and practical advice. The book spans Tony Fadell's journey from early-career product designer to accomplished leader, and offers a treasure trove of insights for anyone trying to run a successful business. Tony's real-world narrative, enriched by his experiences with icons like Steve Jobs is compelling, easy to read and relatable. Each short chapter, ranging from five to 20 pages, tackles real-world challenges – from start-up funding to critical career-life choices and workplace dynamics. What sets this book apart is its blend of personal stories with the wisdom of Silicon Valley, all while advocating for a refreshingly “old-school” approach to leadership and management. *Build* is a must-read for those who want to find real solutions to modern business problems.



## CHECK FRAUD CRIMES ARE “WASHING” AWAY BANK ACCOUNTS

### How Criminals “Wash” Checks

AARP says that most check fraud involves check “washing.” This is when criminals use bleach or acetone to wash away the ink used to write the payee and check amount after stealing it from your mailbox or fishing it from a drop box. Once washed, the check dries, is filled out with new information and deposited at banks or cash-checking shops.

According to AARP, a 60-year-old man had a check for \$235 stolen and cashed for \$9,001.20 – all within 24 hours. It's not just the US either. An Ontario business owner sent a check for \$10,800 to the Canada Revenue Agency to make tax payments for his maple syrup company. Days later, it had been stolen and deposited into another account.

### Prevent Check Fraud With These 6 Tips

1. **Pay Online:** Pay bills online using a private Wi-Fi connection and a secure portal, like through your bank or vendor website.



2. **Mail Safely:** Use the post office for mailing checks; avoid leaving them in personal or outdoor mailboxes.

3. **Use Gel Ink:** Use non-erasable gel ink in blue or black for writing checks; these are harder to erase than ballpoint pen ink.

4. **Collect Mail Daily:** Pick up your mail daily. If away, arrange for collection.

5. **Monitor Your Accounts:** Regularly check your bank account online – a few times a week is best.

6. **Report Incidents Immediately:** Report fraud quickly to your bank and Postal Inspection Service. Most institutions are required to reimburse stolen funds if the theft is reported within 30 days.