onestep
Secure IT Services

2026 VOLUME 2

THE LATEST BYTE

ALL BETS ARE OFF

IN CYBERSECURITY

NO MORE SAFE BETS

If strong cybersecurity isn't a priority for your business, you're taking a massive gamble.

The cyber criminals are hoping you'll bet on not getting breached.

The old rules don't apply anymore. AI has completely changed the game, making attacks sharper and defenses smarter. Every business is now in play in ways we couldn't have pictured a few years back.

The safe bet is gone. Good cybersecurity today is just smart business.

ABOUT ONE STEP SECURE IT

We are an outsourced IT company with over three decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

Our expertise includes Cybersecurity, Managed/Co-Managed IT, Compliance, and Information Security Services.

WE'RE ON THE MOVE

Mark your calendars! One Step Secure IT is attending these upcoming events. Join us and let's talk all things IT and cybersecurity!

CNCDA DEALER DAY

This event offers California dealers an opportunity to meet with lawmakers and advocate for the state's automotive industry.

TUESDAY, APRIL 7TH
SHERATON GRAND SACRAMENTO HOTEL

INNOTECH AUSTIN

This technology and security conference is for IT and security professionals, offering education, networking, and the latest technology and business solutions.

TUESDAY, MAY 12TH
PALMER EVENT CENTER | BOOTH #407

ARIZONA TECHNOLOGY SUMMIT

This B2B conference, with educational presentations and networking sessions, is targeted for the technology and security community.

WEDNESDAY, AUGUST 26TH
PHOENIX CONVENTION CENTER

HIGH-STAKES

GAMBLE ENDS WITH ONE STEP

ALPHA OVERHEAD DOORS CASE STUDY

Stopping a Live Cyber Attack and Becoming a Client in One Day

In late July, Amanda Alquist, owner of Alpha Overhead Doors, noticed something alarming: she was receiving suspicious emails that appeared to come from her own account.

This was an active Business Email Compromise (BEC) attempt. Her existing IT provider dismissed her concerns. Having already lost a significant amount to previous breaches, Amanda was frustrated and worried. She searched online for help and called One Step Secure IT.

The response was...

... immediate.

One Step Secure IT contained the threat that same day, signed Alpha Overhead Doors as a client on the spot, and began securing their systems. Amanda later reflected, "They could tell it was urgent for me and took care of it right away."

What began as an emergency call grew into an ongoing partnership, transforming Alpha Overhead Doors' IT and cybersecurity. The experience redefined Amanda's expectations for service from a Managed Service Provider (MSP).

Company Overview

Alpha Overhead Doors is a family-owned business in Tempe, Arizona, specializing in overhead door installation, repair, and maintenance. Co-owned by Amanda and Justin Alquist, the company has been in operation for seven years and employs approximately 25 people. It serves a mix of commercial and residential clients, including large nationwide accounts.

IT and Security Challenges

Prior to the switch, Alpha Overhead Doors relied on a small IT provider. Service declined after the original owner retired and passed the business on. Multiple incidents highlighted the risks.

In April, a hard drive failure wiped out all accounting data because backups were absent. Around the same time, a breach led to a significant fraudulent withdrawal from the company's bank account. Customers were notified, and some stopped sending emails citing security concerns.

A new employee with IT knowledge shared some concerns about the lack of modern protections. The July BEC attempt became the breaking point.

"If anything like this were to happen that would affect [our client's information], good luck ever becoming their vendor again, right? That's not something they're going to play around with," Amanda said.

Immediate Incident Response

After discovering the BEC attempt and receiving little help from her previous provider, Amanda turned to One Step Secure IT.

Upon Amanda's initial emergency call, the One Step Secure IT team prioritized incident response. Technicians remotely accessed systems to identify and block the BEC activity, secure email accounts, and prevent further unauthorized access. Robust, automated backups were deployed immediately to protect critical data.

Once the attack was contained, One Step began onboarding Alpha Overhead Doors as a full-service client.

Amanda was drawn to One Step Secure IT's family-owned structure, which is similar to her own business, and to the advanced certifications held by multiple team members.

Combined with the rapid, effective response to her emergency, these elements gave her the confidence to move forward immediately and build a partnership that has continued to deliver results.

Delivered Services and Ongoing Improvements

One Step Secure IT's Pro IT Services include proactive monitoring of networks, servers, and endpoints, as well as unlimited remote and on-site support, hardware and software procurement guidance, patch management, and strategic technology planning.

One Step Secure IT's services add advanced protections such as multi-layered endpoint detection and response (EDR), email filtering, phishing simulation training, dark web monitoring, security awareness training for staff, and regular vulnerability assessments.

OPTIMIZED IT AND SECURITY

Amanda describes the team: "Dave Ramsey says you want thoroughbreds, not donkeys. It feels like One Step just has a bunch of thoroughbreds, which is really great. It gives me a huge peace of mind."

Over the next several months, these services delivered tangible upgrades. Systems were optimized for performance, outdated hardware was replaced with reliable business-grade equipment, and security policies were strengthened to support continued growth.

When another computer failed shortly after onboarding, the new backups enabled complete recovery with no data loss. New computers were sourced for the team to ensure the best equipment was provided.

Support tickets are now resolved efficiently through a dedicated help desk. Staff submit requests directly to One Step, and issues are handled promptly without requiring management follow-up.

"When the team has questions, I'm like, you need to call [One Step]. It frees up a lot of time when you don't have to double back. It's been a huge blessing," Amanda said.

Outcomes

With enterprise-grade security now in place, Alpha Overhead Doors can confidently pursue and retain high-value national accounts without fear of losing them over cybersecurity concerns. As Amanda explained,

> *Major customers won't risk a breach through a vendor. We needed big-boy security, so that's what we're doing.*

Months later, satisfaction remains high: "My service so far from One Step has been pretty excellent... I'm really, really, really happy."

Alpha Overhead Doors now operates with reliable, scalable technology and responsive support, empowering the team to focus on business growth instead of IT emergencies.

Ready for Reliable IT and Security?

Alpha Overhead Doors turned an active cyber threat into long-term stability with responsive, professional support. If your business needs a partner that acts fast in a crisis and delivers ongoing peace of mind, reach out to One Step Secure IT for a no-pressure conversation.

(623) 227-1997

www.OneStepSecureIT.com

SECURING THE

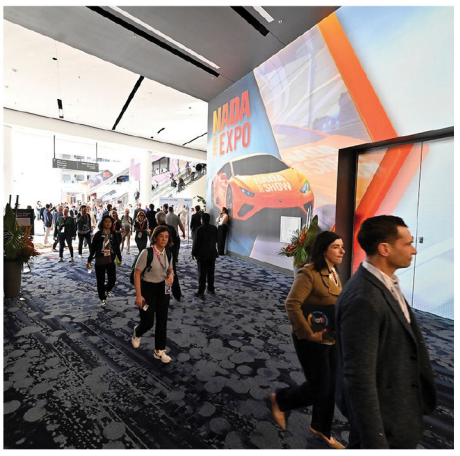
NADA SHOW LAS VEGAS

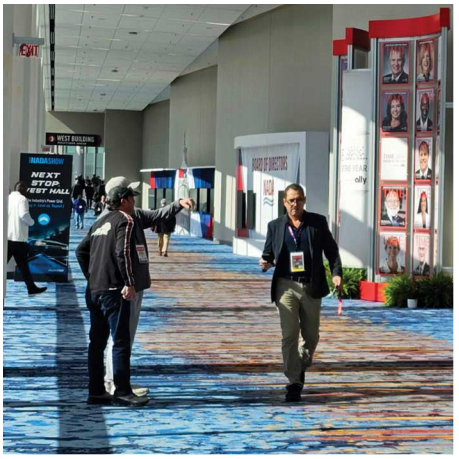
Auto Dealership Leaders Looking to Lessen Cyber Risk

We had a blast meeting auto dealership leaders laser-focused on cybersecurity. Together, we're reducing cyber risk for dealers nationwide.

"My first NADA was epic! Thousands of smart operators solving real problems for auto dealers. Great conversations. Great people. A little nostalgia. A lot of humor. And one thing became clear... This industry isn't slowing down. It's evolving. Grateful to be in the room."

— Dustin Bridgeman,
One Step Secure IT
Technology Consultant





TEXAS TECHNOLOGY SUMMIT HOUSTON

Where Tech Leaders Speak Our Language!

We connected with IT and security pros who get it: strong defenses powered by expert teams make businesses resilient.

We had great talks on how to optimize IT without letting tech become a risk.

FUTURE

One Step Secure IT Hits the Road

Connecting with business and tech leaders to strengthen defenses against cyber threats.

The House Always Wins

Why Cyber Criminals Hold All the Cards & How Businesses Can Change the Game

In a Las Vegas casino, where fortunes are won and lost amid the chime of slot machines and the shuffle of cards, an unassuming fish aquarium hummed quietly.

But this wasn't just any fish tank. It was a smart, IoT (Internet of Things)-enabled device, complete with a connected thermometer that monitored water temperature, salinity, and feeding schedules. Little did the casino know that this aquatic gadget would become the unlikely gateway to a major cyber attack.

Hackers, ever opportunistic and scanning for weak links, discovered a vulnerability in the thermometer's firmware or its outdated software, which is common in many IoT devices with default credentials or unpatched flaws.

With a few clever exploits, they gained unauthorized access to the device and, from there, they pivoted laterally across the systems. Moving stealthily through connected infrastructure until they located their real prize: A sensitive database containing details on the casino's high-roller clients. This included names, gambling habits, contact information, credit details, and other personally identifiable information.

The attackers exfiltrated over 10 gigabytes of this valuable data. To avoid triggering alarms, they routed the massive transfer back through the fish tank's internet connection itself, disguising the outflow by using protocols typically reserved for streaming audio or video.

By the time the casino called in cybersecurity firm Darktrace, the data had already been leaking for some period.

"This was a clear case of data exfiltration," notes the Darktrace report, "but far more subtle than typical attempts at data theft."

Even a humble aquarium sensor, when connected without proper network segmentation, firewalls, or monitoring, can provide attackers with a perfect, low-profile entry into sensitive environments.

The House Always Wins
Why Cyber Criminals Hold the Upper Hand

In the high-stakes world of casinos, the adage "the house always wins" is a fundamental truth, baked into the odds and designed to ensure long-term profitability for the establishment.

In the world of cybersecurity, cyber criminals are the "house," and business owners are the gamblers at the table. Instead of betting chips, business owners are betting that their security systems will keep their company safe. But sophisticated cyber criminals can routinely outmatch these defenses.

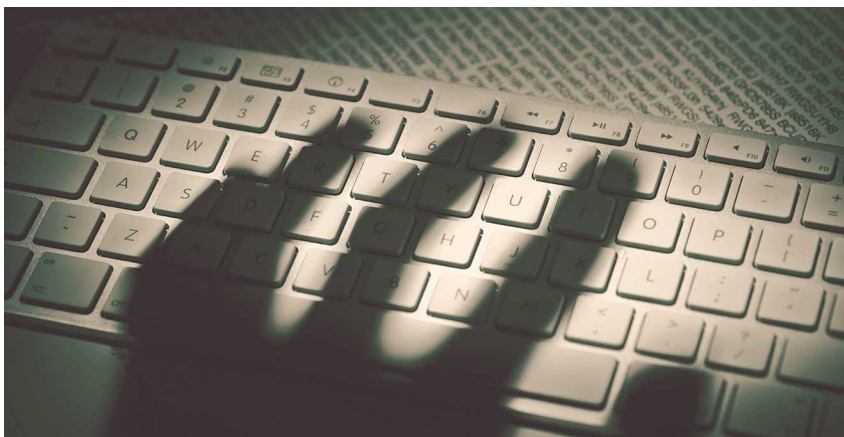
Unlike a night at the blackjack table, this isn't a game; the stakes are more significant, and the losses can stretch beyond money lost. Businesses frequently end up "playing" whether they want to or not by operating a business in today’s technology-reliant environment.

Cyber criminals operate with inherent advantages that stack the deck against even the most prepared organizations. They strike from the shadows, often anonymously and across borders, exploiting resources, technology, and motivation.

While businesses must defend every entry point 24/7, attackers only need to find one weakness to succeed. Attackers increasingly use "double extortion" tactics, not only encrypting data but also threatening to leak it publicly, forcing hands even when backups exist. The rise of "ransomware-as-a-service" (RaaS) kits on the dark web lowers the barrier for entry, allowing even novice hackers to launch professional-grade attacks.

Cyber criminals don't face regulatory hurdles, budget constraints, or ethical dilemmas; they innovate freely, probing for vulnerabilities in everything from outdated software to human error.

For business owners, the result is a perpetual gamble where ignoring the risks can lead to bankruptcy, legal liabilities, or loss of customer trust. When attackers win, businesses pay, not just in ransoms, but in eroded confidence and stalled growth.



Protecting Your Business
Practical Tips to Shift the Odds

Fortunately, while the house may hold advantages, smart strategies can level the playing field. The key is proactive defense, treating cybersecurity not as a one-time expense but as an ongoing investment in your business's future.

Train Your Team
Conduct regular phishing simulations and cybersecurity workshops to educate employees on spotting suspicious emails, avoiding shady links, and reporting incidents promptly. Make it engaging by using gamified training platforms to keep participation high.

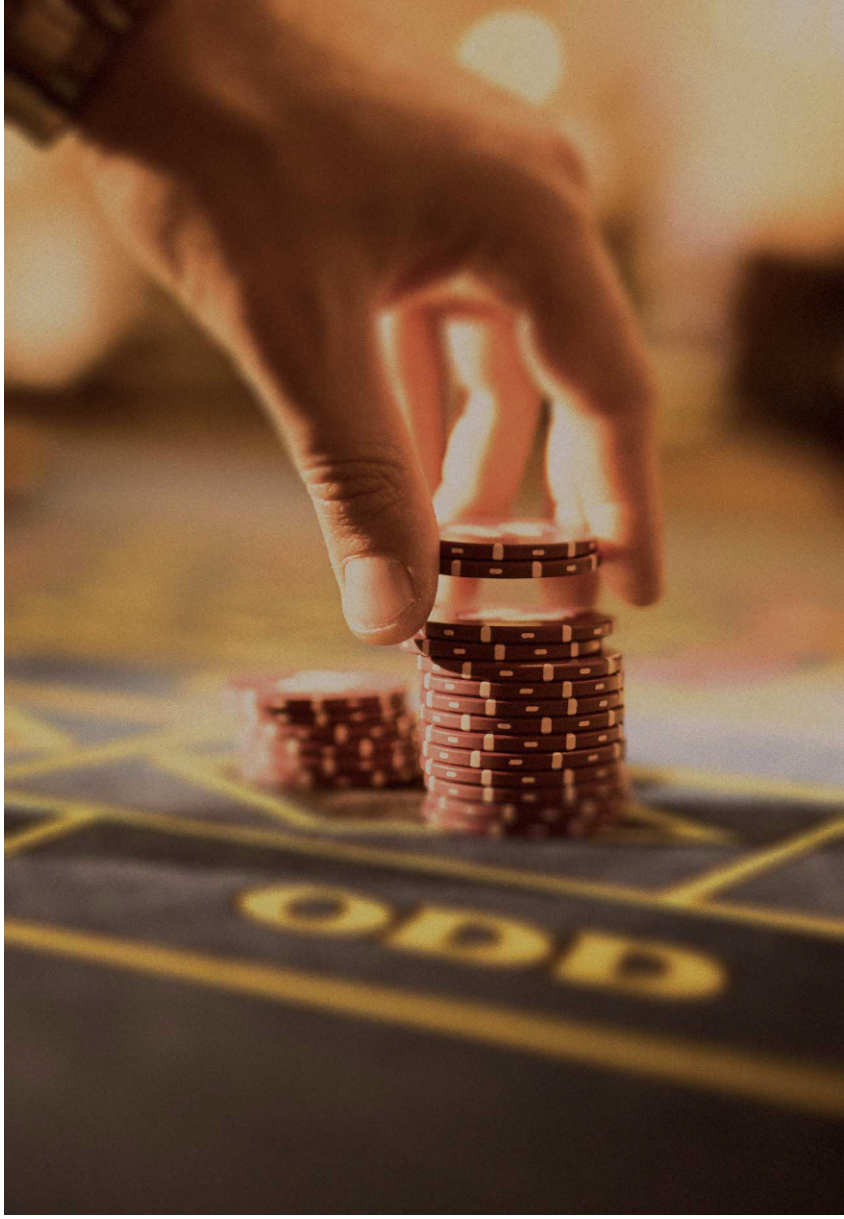
Keep Software and Systems Updated
Outdated software is a hacker's best friend. Automate patch management for operating systems, applications, and IoT devices to quickly close known vulnerabilities. Schedule regular audits to ensure nothing slips through the cracks.

Back Up Data and Test It
Ransomware preys on desperation. Maintain offline or air-gapped backups (not connected to your main network) and test restores quarterly. Follow the 3-2-1 rule: three copies of data on two different media types, with one offsite.

Segment Your Network and Monitor Activity
Don't let a breach in one area spread like wildfire. Use network segmentation to isolate critical systems, and deploy endpoint detection and response (EDR) tools to flag unusual behavior in real time.

Develop an Incident Response Plan
Hope for the best, but plan for the worst. Create a step-by-step playbook outlining who to contact (e.g., legal counsel, insurers, authorities) and how to contain damage. Run tabletop exercises to simulate attacks and refine your approach.

These steps aren't guaranteed protection because no defense is, but they significantly reduce risk and demonstrate due diligence, which can mitigate legal repercussions post-breach.



When to Call in the Pros
Guidance to Get on the Right Track

Many business owners juggle countless priorities and lack the time or expertise to dive deep into cybersecurity. That's where seeking help from professionals can put you on the right track and provide essential guidance on where to start.

Managed Security Service Providers (MSSPs) can conduct a thorough audit of your systems, identifying blind spots you might miss. They'll prioritize high-impact actions based on your industry and size, ensuring your defenses align with emerging threats.

By arming yourself with knowledge, tools, and allies, you can transform from a gambler into a guardian of your enterprise. Remember, the house may always aim to win, but with vigilance, businesses can rewrite the rules and come out ahead. After all, in this casino of cyber risks, the smartest players know when to bring in a card counter.

onestep
Secure IT Services

Stop **Gambling** with **Cybersecurity**

Start Tackling the Risks Facing Your Business with the **Cybersecurity Risk Management eBook**

Business leaders can't afford to gamble with "We're too small to be hacked." In reality, 43% of cyber attacks target small businesses, yet only 14% are prepared (per Accenture's cyber crime study).

One Step Secure IT's eBook *Cybersecurity Risk Management: Frameworks, Threat Landscape, and Best Practices* is your guide to managing the risks created by increasing cyber attacks, safeguarding business operations, and protecting your reputation and sensitive data. Criminals target easy victims. Don't be one.

The experts at One Step Secure IT have created a straightforward Cybersecurity Risk Management eBook just for business leaders, and it's completely free. Download it today.

Is Your **Business** Exposed?

The cybersecurity experts at One Step Secure IT are providing the perfect onramp to getting a clearer picture of where you're taking a gamble with your security.

Together, we'll take a look at:

- Industry benchmarking to see how your cybersecurity measures compare to industry standards
- What your business is doing right to stay secure, and where hidden risks might still threaten your operations
- How tailored best practices from our cybersecurity experts can strengthen your defenses

Take the First Step Toward a **More Secure Business**

Schedule your Business Exposure Snapshot at **www.OneStepSecureIT.com/tlb-snapshot** or scan:

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

onestep
Secure IT Services

www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT