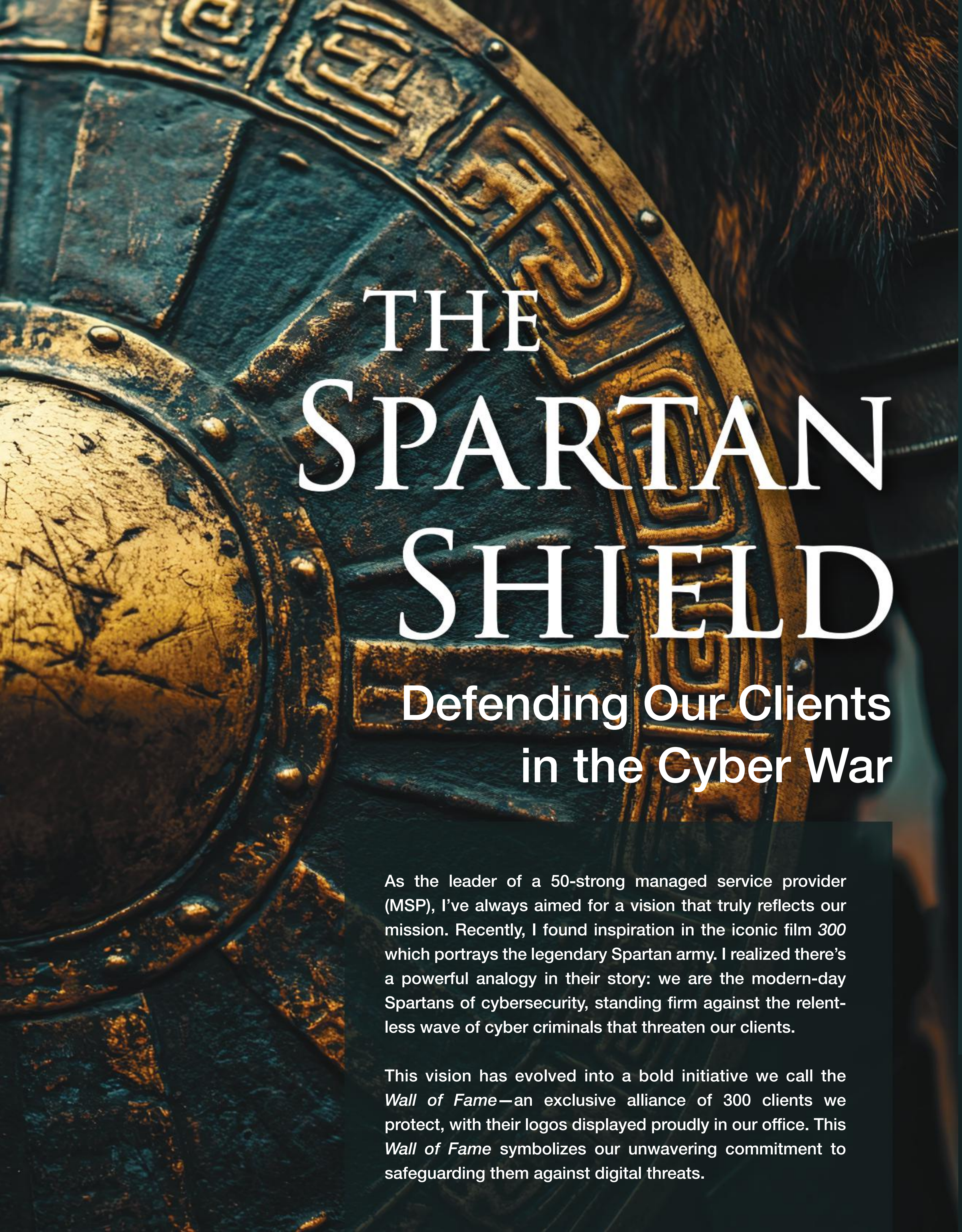
CYBER SPARTANS

THE LATEST BYTE

STRONG TEAMS, STRONG SHIELDS

ONE STEP SECURE IT

2025 VOL 3



THE SPARTAN SHIELD

Defending Our Clients in the Cyber War

As the leader of a 50-strong managed service provider (MSP), I've always aimed for a vision that truly reflects our mission. Recently, I found inspiration in the iconic film *300* which portrays the legendary Spartan army. I realized there's a powerful analogy in their story: we are the modern-day Spartans of cybersecurity, standing firm against the relentless wave of cyber criminals that threaten our clients.

This vision has evolved into a bold initiative we call the *Wall of Fame*—an exclusive alliance of 300 clients we protect, with their logos displayed proudly in our office. This *Wall of Fame* symbolizes our unwavering commitment to safeguarding them against digital threats.

Like the Spartans at Thermopylae, our strength lies not in sheer numbers but in discipline, strategy, and unity. In today's digital battlefield, tools like firewalls, antivirus software, and intrusion detection systems are just that—tools.

A spear in untrained hands is ineffective; a shield is useless without a capable warrior behind it. Cyber criminals, like the opponents in the film, are clever and relentless, exploiting even the smallest vulnerabilities. That's why our team members—skilled engineers, analysts, and technicians—undergo rigorous training to master these tools. They don't merely implement solutions; they deploy them with expertise, adapting to emerging threats in real time.

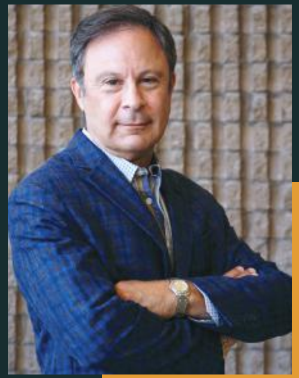
Even the best warriors need effective leadership. Our "generals"—the senior strategists and incident response leaders—bring decades of experience to the battlefield. They don't just respond to attacks; they anticipate them, developing proactive defenses that strengthen our clients' digital fortresses. They ensure our team operates efficiently, minimizing risks and maximizing resilience. This blend of cutting-edge tools, expert operators, and strategic oversight forms the foundation of our Spartan approach.

The *Wall of Fame* is more than just a display or a club—it's a pledge. Each logo symbolizes a client we've committed to protecting, a business we've shielded from ransomware, phishing attacks, and data breaches. It is a testament to our dedication to serving as their first line of defense against chaos in an environment where cyber crime costs businesses trillions of dollars annually; joining the 300 means entrusting your cybersecurity to a team that adheres to the Spartan code: courage, discipline, and sacrifice.

onestep
WALL OF FAME
CLIENTS WE PROTECT
" The Spartans are the equal of any men when they fight as individuals; fighting together as a collective, they surpass all other men. "

As we build this wall, client by client, we invite businesses to join us—not just as clients but as partners in a shared mission. Together, we can create a legacy of resilience, demonstrating that with the right warriors, effective leaders, and unwavering resolve, no cyber army can breach our defenses. Join us and be recognized as one of the esteemed 300 on the *Wall of Fame*.

A WORD FROM OUR CEO
SCOTT KREISBERG



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, Information Security, and Compliance Services.

Cybersecurity is becoming a battlefield where no business, big or small, is safe. While headline-grabbing breaches at major companies like Target and Equifax expose millions of records, cyber criminals use the same tactics—phishing, unpatched vulnerabilities, and supply chain attacks—to target small businesses with fewer defenses. These smaller breaches rarely make the news.

BREACHES & SHIELDS

KEY TAKEAWAYS FROM LOST CYBER BATTLES

Every breach is a lesson in resilience. We're going to take a look at six infamous "lost cyber battles" to uncover what went wrong and how business owners can fortify their defenses. These stories—from ransomware to supply chain attacks—offer practical tools and strategies to build stronger teams and more effective shields.

YAHOO'S RECORD-BREAKING BREACH *AUG 2013*

Yahoo's 3 billion account breach, revealed in 2017, stemmed from weak password hashing and outdated systems.

What Went Wrong?
Legacy systems and poor credential protection went unmonitored.

Lesson
Modernize security and monitor for breaches.

Tools
Enforce multi-factor authentication (MFA) and security information and event management (SIEM) systems to detect anomalies.

TARGET'S HVAC HACK *JAN 2014*

Hackers infiltrated Target through stolen HVAC vendor credentials, accessing 40 million credit card numbers and 70 million customer records. Poor network segmentation allowed free movement, costing $300M.

What Went Wrong?
Target underestimated third-party risks and lacked isolated networks.

Lesson
Vet vendors rigorously and limit their access.

Tools
Implement third-party risk management platforms and network segmentation to contain breaches. Regular vendor audits strengthen your supply chain.

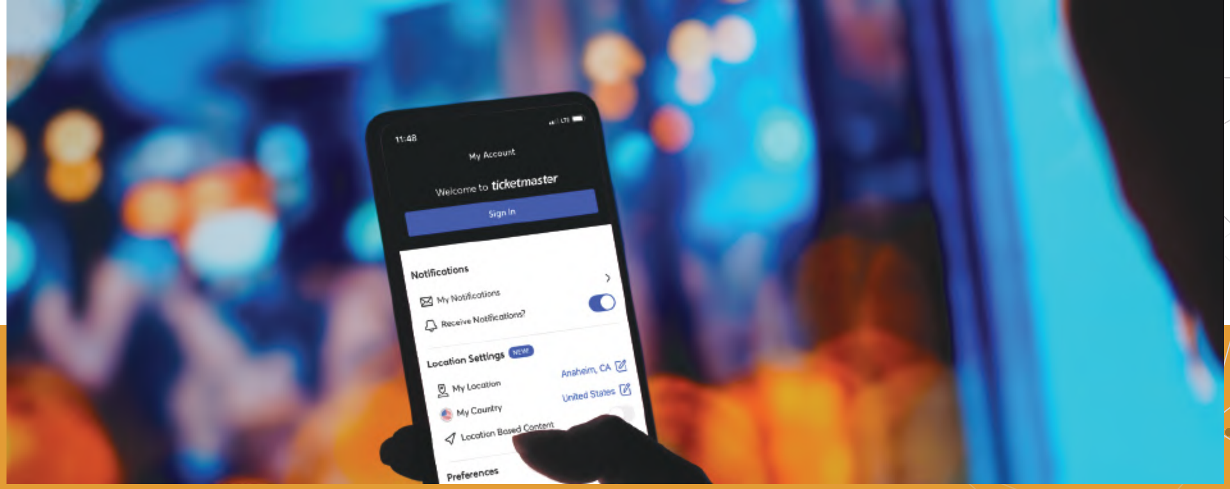
WANNACRY RANSOMWARE RAMPAGE *MAR 2017*

WannaCry exploited an unpatched Windows SMB flaw, infecting 200,000+ systems across 150 countries, crippling hospitals, and costing $4B. A patch was available months earlier.

What Went Wrong?
Delayed patching and weak endpoint security fueled the chaos.

Lesson
Patch promptly and monitor endpoints.

Tools
Use automated patch management and endpoint detection and response (EDR) tools to detect and isolate threats. Schedule weekly patch cycles to stay ahead.



EQUIFAX'S PATCHING FAILURE *SEP 2017*

Equifax failed to address a known vulnerability in Apache Struts, an open-source framework for developing Java-based web applications, enabling hackers to steal the personal data of 147 million Americans, including Social Security numbers, and resulting in $700 million in settlements.

What Went Wrong?
Slow patching and weak access controls exposed sensitive data.

Lesson
Prioritize patching and restrict access.

Tools
Use automated vulnerability scanners and zero-trust access controls to limit exposure. Test patches in a sandbox environment to ensure compatibility.

TICKETMASTER'S SCRIPT ATTACK *JUN 2018*

Hackers injected malicious JavaScript into a Ticketmaster chat widget, stealing 40,000 customers' payment details over months.

What Went Wrong?
Unvetted third-party scripts and lax web security enabled the attack.

Lesson
Scrutinize external code and secure web applications.

Tools
Deploy content security policies (CSP) to block unauthorized scripts and web application firewalls (WAFs) to filter malicious traffic. Vet all third-party integrations before deployment.

SOLARWINDS SUPPLY CHAIN ATTACK *DEC 2020*

Malicious code was injected into SolarWinds updates, compromising 18,000 organizations, including U.S. agencies. It went undetected for months.

What Went Wrong?
Poor supply chain vetting and lack of anomaly detection enabled stealthy attacks.

Lesson
Verify your vendors' security and monitor your network for unusual activity.

Tools
Adopt supply chain risk management platforms and anomaly detection tools to flag suspicious behavior. Implement zero trust architecture to prevent lateral movement.

Forging Your Cyber Shield

These breaches highlight that cybersecurity hinges on vigilant teams and robust tools. Business owners must prioritize patching, employee training (e.g., phishing simulations), and third-party oversight. Invest in MFA, SIEM, EDR, and zero trust to create layered defenses. Regular audits and attack simulations keep your team sharp. When it comes to cybersecurity, preparation is your strongest weapon—learn from these losses to build an unbreakable shield.

WHAT'S IN YOUR CYBERSECURITY TOOLBOX?

In 2025, cyber threats evolve faster than ever, putting your business's data, operations, and reputation at risk from a single breach. Cyber threats are evolving at an alarming rate, targeting everything from sensitive data to operational systems. Without the right defenses, a cyber attack can damage your reputation and lead to significant financial losses. So, how can you ensure your business is protected in 2025? It starts with having the right tools in your cybersecurity toolbox—but tools alone aren't enough.

A well-rounded cybersecurity toolbox is the foundation of a strong defense, covering everything from securing your network to monitoring for threats and ensuring quick recovery after an incident. The graphic on the next page outlines the essential tools your business needs to stay ahead of cyber threats in 2025. It's a list designed to help you identify gaps in your current setup and take action to strengthen your security. However, having the best tools is only part of the equation. To truly protect your business, you need skilled security professionals who can deploy, manage, and optimize these tools effectively.

Tools Are Not Enough

Even the most advanced cybersecurity tools can fall short if they're not used properly. Misconfigurations, outdated systems, or lack of expertise can leave vulnerabilities that attackers are quick to exploit. Security professionals bring the knowledge and experience needed to ensure your tools are implemented correctly, tailored to your business's unique needs, and continuously monitored for maximum effectiveness. They can also provide strategic guidance, helping you stay ahead of emerging threats and ensuring your defenses evolve as quickly as the challenges do.

Why It Matters Now

The stakes have never been higher. A single vulnerability can be exploited in minutes, leaving your business exposed. By combining a comprehensive toolbox with the expertise of security professionals, you're not just reacting to threats—you're preventing them. This approach ensures your business can operate with confidence, knowing you're prepared for whatever challenges come your way.

The Cybersecurity Toolbox Every Business Needs in 2025

Perimeter Protection

Network Firewall
Web Application Security
Intrusion Prevention

Access & Identity Management

Multi-factor Authentication
Single Sign-On
Priviledge Access Management

Monitoring & Visibility

Log Aggregation
Network Traffic Analysis
Endpoint Monitoring

Threat Intelligence & Incident Response

Threat Intelligence Feeds
Security Automation
Forensics Tools

Vulnerability & Patch Management

Vulnerability Scanning
Automated Patch Deployment
Asset Inventory

Endpoint Protection

Endpoint Detection & Reponse
Mobile Device Management
Application Control

Data Protection & Compliance

Data Loss Prevention
Email Security
Encryption Tools

Automation & AI-Based Defenses

Behavioral Analytics
Automated Threat Hunting
Anomaly Detection

Training & Awareness Platforms

Security Awareness Training
Phishing Simulations

Backup & Recovery

Automated Backup
Disaster Recovery
Immutable Storage

Ready to Build Your Toolbox?

Don't leave your business vulnerable to cyber threats. The right cybersecurity tools, paired with expert support, can make all the difference between a secure future and a costly breach. Want to ensure your tools are up-to-date and utilized effectively? Partner with One Step's trained security professionals to secure your business today.

Give us a call at 623-227-1997 to get the Cybersecurity Toolbox your business needs to stay safe in 2025 and beyond!

Held Hostage

A ONE STEP SECURE IT CASE STUDY

How One Step freed Hooks Lincoln from their IT nightmare.

For months, the team at Hooks Lincoln, a trusted, family-owned auto dealership in Fort Worth, Texas, felt like they were being held hostage, not by ransomware or hackers—but by their own Managed Service Provider (MSP).

Things had started out fine. The dealership didn't have an internal IT team, so they turned to an outside provider to help manage and secure their systems. But by mid-2024, the relationship had turned toxic. Requests were ignored. Support dwindled. And when Hooks Lincoln finally decided to part ways, the real nightmare began.

The MSP flat-out refused to cooperate. They wouldn't extend the contract—not even by a month. Worse, they refused to uninstall their own security tools, leaving Hooks Lincoln's systems in limbo. With 41 endpoints exposed, and no in-house IT staff to intervene, the dealership was staring down the barrel of a potential data breach.

"We got in a really tough spot," said Director of Operations at Hooks Lincoln, Hunter Greenwood.

They were stuck. Trapped. And time was running out.

Enter the Rescue Team: One Step Secure IT

In August 2024, with pressure mounting and operations at risk, Hooks Lincoln found their lifeline: One Step Secure IT.

From day one, One Step treated the situation like the urgent crisis it was. Their "No Hostage Guarantee" wasn't just a promise—it was a mission. Leading the charge was Tim Derrickson, CISSP and Director of IT & Security Services. Tim tackled the mess head-on, untangling contracts, and prying control back from the uncooperative MSP.

"It was like night and day," Hunter said. "Tim really saved the day."

Meanwhile, Peyton Hitchcock, Hooks Lincoln's newly assigned Network Administrator, got to work rebuilding their IT environment from the ground up.

If Hunter runs into any technology issues at the dealership, "I can just call Peyton and figure it out. It's always A1 service."

From Chaos to Control

One Step didn't just plug holes—they built a secure technology environment that is prepared for growth into the future.

Their tech team traveled to Fort Worth, installed a centralized server, and brought all 41 devices—31 desktops and 10 mobile units—under a secure, centrally managed system.

They deployed:

- 🔒 24/7 Security Operations Center (SOC) monitoring
- 🔒 Managed Detection and Response (MDR)
- 🔒 Zero Trust Application Whitelisting
- 🔒 Full Antivirus Protection, Dark Web Monitoring, and Cloud Backups

Suddenly, Hooks Lincoln wasn't just operational—they were compliance-ready for Cyber Liability Insurance and armed with a top-tier cybersecurity strategy.

A True Partnership

With One Step on board, Hunter describes a complete 180° shift: "I've had truly zero issues."

Peyton quickly became more than just support—he was a strategic ally, offering fast answers, clear direction, and peace of mind. One Step's Virtual CIO (vCIO) now helps the dealership plan for the future, mapping out upgrades and security measures in quarterly briefings.

"The planning aspects are lightyears ahead of what we used to have."

Hunter no longer loses sleep over what might be hiding in his network. "I don't need to know everything—y'all have my back covered."

The Bottom Line

Hooks Lincoln was trapped in a dangerous situation—vulnerable, unsupported, and left in the dark by an MSP that stopped caring.

But One Step Secure IT turned their situation around. With 38+ years of experience, a battle-tested team, and a commitment to never leaving a client behind, they turned a high-stakes IT crisis into a story of strength, stability, and partnership.

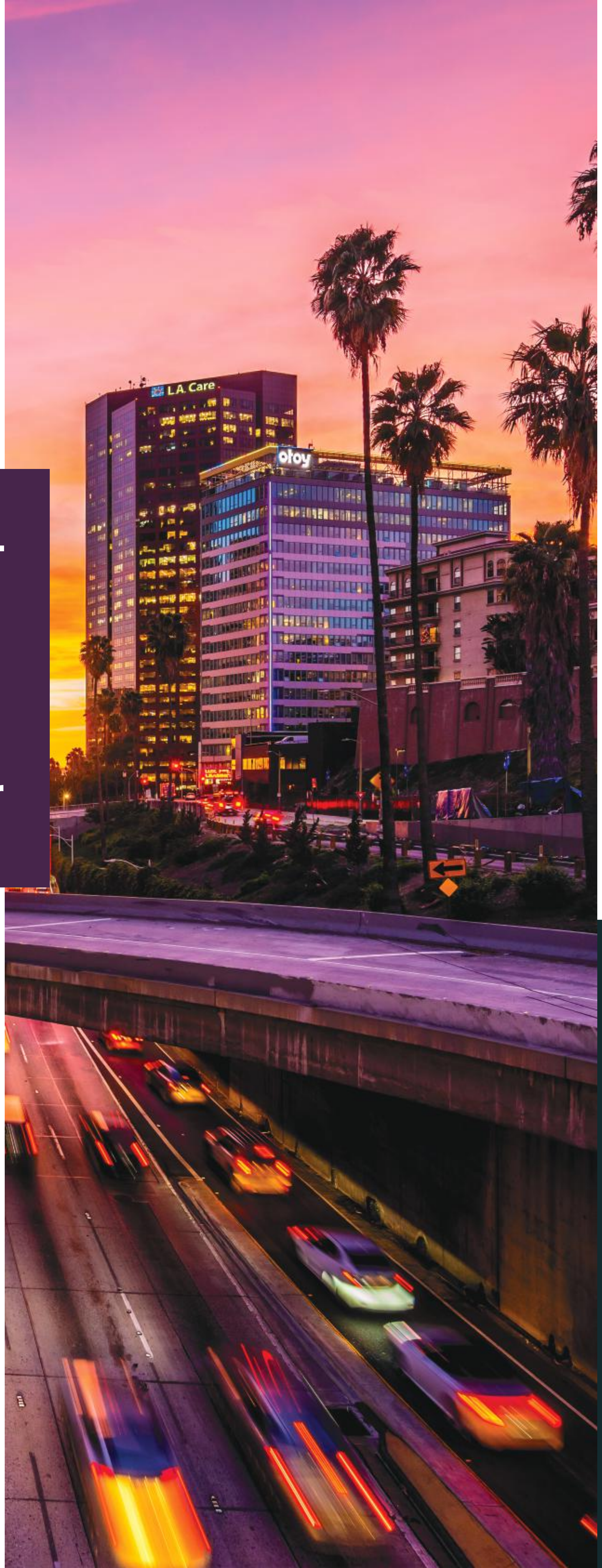
Today, Hooks Lincoln stands stronger than ever—protected, supported, and empowered by a partner they can trust.

PRESS RELEASE

One Step Secure IT Partners with CNCDA as a Licensed IT Vendor

Phoenix, Arizona
One Step Secure IT proudly announces its licensed vendor partnership with the California New Car Dealer Association (CNCDA), which offers managed information technology (IT) services to CNCDA member auto dealerships. This collaboration marks a milestone in One Step's pursuit of ensuring operational resilience across the automotive industry.

“We are proud to have One Step as a new official licensed vendor for our association. Their managed IT offerings will not only assist our dealers in providing the best service to their customers, but they will also help CNCDA provide enhanced association benefits and opportunities to our members. We are happy to have them join us,” said Brian Maas, CNCDA President.



One Step provides IT and additional services throughout the United States, giving dealerships access to a full team of experts to help them optimize and secure their business technology.

“Teaming up with the CNCDA exemplifies our dedication to protecting auto dealerships across the nation," stated Scott Kreisberg, Founder and CEO of One Step Secure IT. "With over 35 years of experience, One Step Secure IT empowers dealerships to streamline IT operations and safeguard their assets. Our goal is to equip auto dealerships with the necessary resources and expert knowledge to secure their financial interests and succeed in a competitive market.”

CONNECTING WITH CALIFORNIA DEALERS

Our One Step Secure IT team had the privilege of attending **CNCDA's Dealer Day** this March! It was a fantastic opportunity to connect with auto dealership leaders from across California.

We enjoyed great conversations about how dealerships are strengthening their security and taking smart steps to better protect their data.

Photography by: Kevin Fiscus Photography at kevin@kevinfiscus.com www.kevinfiscus.com

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