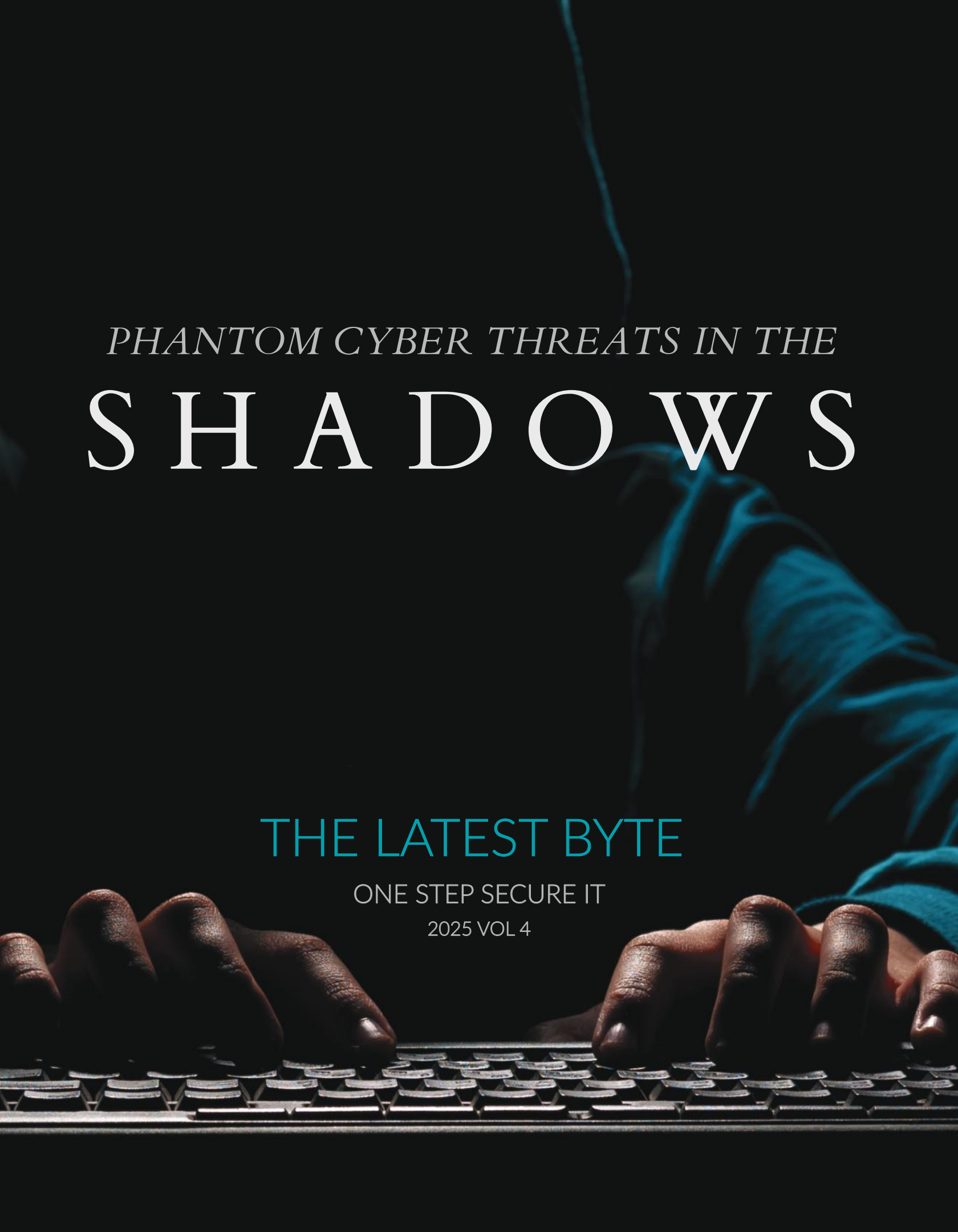


PHANTOM CYBER THREATS IN THE SHADOWS

THE LATEST BYTE

ONE STEP SECURE IT

2025 VOL 4

PHANTOM CYBER THREATS IN THE SHADOWS

October marks both Halloween and Cybersecurity Awareness Month, a fitting convergence that highlights the hidden dangers of operating a business. At One Step Secure IT, we are committed to protecting businesses from cyber risks. This issue of *The Latest Byte* delves into the critical risks facing organizations, from outdated legacy systems to sophisticated hackers to insidious phishing attacks, while providing actionable insights and strategies to fortify your organization's security.

Cybersecurity Awareness Month Champion

At One Step Secure IT, we're proud to be recognized as an official *Cybersecurity Awareness Month Champion*, joining a national effort to equip businesses with the knowledge and tools to stay safe online.

Cybersecurity Awareness Month, held every October since 2004, is a global initiative to promote cybersecurity, co-led by the National Cyber Security Alliance and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

This year's theme is Stay Safe Online, and it's built around the Core 4:

1. Use strong passwords and a password manager
2. Turn on multifactor authentication
3. Recognize and report phishing scams
4. Keep your software up to date

These are high-impact actions that reduce risk, especially for small and midsize businesses navigating a rising tide of cyber threats.

This October and into the new year, let's go beyond the basics. Let's get intentional about protecting your business, your people, and your peace of mind.

ABOUT US

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.

One Step's expertise includes Cybersecurity, Managed/Co-Managed IT, Information Security, and Compliance Services.

HAUNTED BY LEGACY SYSTEMS

[START]

In the early 1980s, I was just getting started in the world of technology. My days were spent in a garage building computers and untangling wires. I launched my first business providing tech solutions to retailers who were still using dot matrix printers and green-screen terminals. Back then, we called these systems "reliable."

Fast forward 40 years, and I'm now leading a cybersecurity and IT services company serving clients across a range of industries. But one challenge has followed me through every stage of this journey: legacy systems.

What once felt like a smart investment has, for many businesses, become a hidden anchor—dragging down innovation, increasing cyber risk, and stalling growth. As someone who's been in the trenches, I understand why businesses hang on to the old. It's familiar. It works. And it feels safer than diving into the unknown.

...BUT I ALSO KNOW THIS: IF WE DON'T EVOLVE, WE RISK BEING LEFT BEHIND.

These aging infrastructures, built on obsolete code or hardware, lack the flexibility to integrate with cutting-edge tools like AI, cloud computing, or real-time analytics, slowing down development cycles and hindering competitive advantage. Modernizing without disrupting operations is a delicate balance, but it's achievable through strategies like incremental migration, where systems are updated in phases to minimize downtime.

I want to demystify modernization and show that you don't have to choose between innovation and stability. There's a path forward that keeps your business secure, competitive, and ready for what's next.

What Are Legacy Systems? And Why Are They Still Here?

Legacy systems are outdated hardware or software platforms that are still in use despite newer alternatives being available. Consider Windows 7, mainframes that run COBOL, or ERP software that hasn't received updates in a decade. These systems often perform critical functions, which is why businesses are hesitant to part with them.

According to a 2024 report by Gartner, 67% of mid-sized businesses still rely on at least one core legacy application to run daily operations. The reasons include:

- High switching costs
- Fear of downtime
- Lack of in-house expertise
- "If it ain't broke, don't fix it" mentality

But here's the problem: Just because it isn't "broken" doesn't mean it isn't a liability and a security risk.

THE SILENT KILLERS

How Legacy Systems Undermine Innovation

Security Vulnerabilities

Legacy systems often lack modern security protocols. They aren't built to withstand today's sophisticated cyber threats, making them easy targets for ransomware, data breaches, and malware.

A 2025 study by Cybersecurity Ventures found that 78% of ransomware attacks in the first quarter targeted organizations running outdated software platforms.

Integration Roadblocks

Modern software stacks are designed to be modular and API-driven. Legacy systems, on the other hand, often require custom integrations or manual workarounds, leading to inefficiencies and data silos.

Innovation Bottlenecks

When IT departments are busy maintaining outdated systems, they have less time and fewer resources to invest in innovation. This directly impacts digital transformation, automation, and AI adoption.

Talent Drain

New tech talent doesn't want to work with outdated technology. This makes it harder to recruit and retain skilled developers, engineers, and analysts.

Compliance Risks

Older systems may not meet current regulatory standards such as GDPR, HIPAA, or PCI DSS 4.0. This can lead to audits, fines, and reputational damage.

Why Businesses Are Afraid to Let Go

Modernization is intimidating. The risks of downtime, data loss, and budget overruns keep many decision-makers frozen in place. According to a 2024 International Data Corporation (IDC) survey, 58% of CIOs said fear of disrupting business continuity was the biggest barrier to digital transformation.

But sticking with outdated systems has its own hidden costs:

- $ Lost revenue from downtime
- $ Inability to scale operations
- $ Customer churn due to poor user experiences
- $ Missed opportunities from AI, cloud, and automation

How to Modernize Without Disrupting Business Continuity

1. Start with a System Audit

Begin by identifying which systems qualify as legacy and evaluating their associated risks and value to the organization. Develop a technology map that categorizes these systems based on three key criteria: business criticality, security risk, and integration complexity. This approach enables a clear understanding of each system's importance to business operations, potential vulnerabilities, and the challenges involved in integrating them with modern infrastructure.

2. Build a Modernization Roadmap

Rather than abruptly ripping and replacing outdated systems, adopt a phased approach to upgrading or replacing them, prioritizing critical factors such as security vulnerabilities, high maintenance costs, and limited vendor support. Focus on modernizing one component at a time, gradually migrating data and replacing legacy functions while ensuring core operations remain intact and improvements are rolled out in a controlled manner. Ultimately, modernize step by step and ensure a smooth transition.

3. Build APIs Around Legacy Systems

Instead of pursuing full system replacements, begin by developing Application Programming Interfaces (APIs) to enable seamless communication between legacy platforms and modern tools. These APIs act as bridges, connecting outdated infrastructure with new applications to enhance flexibility while maintaining operational continuity. By integrating new technologies through APIs, you can improve the flexibility of your existing infrastructure without causing disruptions.

4. Embrace Hybrid Environments

Many businesses achieve success by integrating on-premise and cloud solutions during the transition from legacy systems. This hybrid approach minimizes downtime and provides teams with ample time to adapt to new technologies, ensuring a smoother and more effective modernization process while maintaining operational stability.

5. Prioritize System Connectivity

To make upgrading easier, focus on connecting outdated systems to new ones without disrupting daily work. Use tools like middleware and API platforms, which act like translators to help old and new systems "talk" to each other. This lets you update things gradually in the background while keeping everything running smoothly.

6. Engage and Inform Key Decision-Makers

To ensure a successful system upgrade, involve cross-functional teams from the start, including executives, department leaders, and IT staff. Clearly explain the risks of keeping outdated systems and highlight the advantages of modernization. This early collaboration builds understanding and support, paving the way for a smoother transition.

7. Partner with Experts

If your team doesn't have experience with legacy system upgrades, partner with a Managed Service Provider (MSP) or IT consultant who specializes in gradual modernization. You don't need to tackle it alone—their expertise can guide a smooth, step-by-step transition.

The Competitive Edge of Modern Tech Stacks

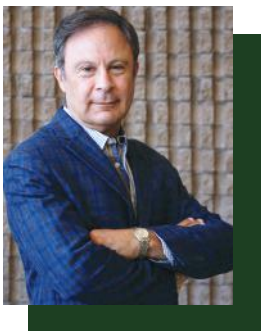
Proactively modernizing technology stacks provides companies with a competitive edge by enabling faster go-to-market times, real-time data analytics, scalable cloud infrastructure, enhanced cybersecurity, and higher satisfaction for both employees and customers. According to a 2025 Deloitte report, digitally mature companies leveraging modern tech stacks are 23% more profitable and 34% more likely to successfully launch new products, underscoring the significant advantages of staying ahead in the digital landscape.

Final Thoughts: Innovation Demands Bold Moves

Legacy systems may feel like a safe bet, but they're quietly stalling innovation and increasing risk. Whether you're in retail, finance, or another fast-moving industry, modernization is no longer optional.

The good news? You don't have to rip everything out to move forward. With a phased, flexible strategy—and the right mix of APIs, microservices, and modern platforms—you can evolve at your pace, without putting your business on hold. Modernizing your tech stack isn't about chasing trends, it's about staying in business and staying competitive.

Don't wait for disruption to force your hand. Work with One Step Secure IT to design a roadmap that leads your business to a more profitable and secure IT environment.



INSIGHTS FROM

Scott Kreisberg

CYBERSECURITY MONSTERS

Risks Every Business Leader Must Confront

As Halloween approaches, the season's tales of lurking monsters serve as a timely metaphor for the shadowy threats in cybersecurity. These digital risks, like phishing, ransomware, tracking, and privacy invasions, weak password practices, and dormant accounts, can emerge unexpectedly, disrupting operations and eroding trust.

For business leaders, the cyber risks are real and they pose a threat year round, not just during the Halloween season. This article explores each "monster," providing strategic insights to safeguard your organization in an era of escalating cyber risks. Monsters aren't hiding under the bed; they might just be lurking within your business network...

The Phisherman

Luring Victims with Deceptive Bait

Much like a spectral fisherman casting lines in the mist, phishing attacks bait unsuspecting users with deceptive urgency. Accounting for over 90% of data breaches, according to 2024 industry reports, these threats exploit human psychology to extract credentials or install malware. Spear-phishing personalizes attacks using social media intel, while whaling targets executives with fabricated high-stakes scenarios, such as merger alerts.

Mitigation requires layered strategies: simulated training to build employee awareness, AI-driven email filters to spot domain anomalies, and zero-trust models to verify all accesses. Quarterly incident reviews can halve breach success rates, per Deloitte data, protecting financial stability and reputation.

The Ransomwolf

The Hunter Looking for Payment

Ransomware strikes suddenly, encrypting data and extorting payments, averaging over $1 million in 2024, according to Chainalysis. The fallout includes operational halts, legal repercussions, and leaked sensitive information, amplifying enterprise vulnerabilities.

Countermeasures include secure, offline backups for swift restoration, network segmentation to isolate infections, and machine learning- based EDR for real-time threat containment. Robust incident response plans, bolstered by cyber insurance, address legal and communication needs. Work to avoid falling victim by implementing robust cybersecurity measures like regular data backups, employee training on phishing detection, and up-to-date antivirus software.

The Computer Cookie Goblin

Sneaking Through Privacy Cracks

Tracking cookies and privacy breaches sneakily collect data for ads or illegal sales, risking multimillion-dollar fines under GDPR or CCPA. Cisco's 2024 surveys show 75% of respondents won't buy from companies they don't trust with their data.

Defenses involve browser extensions for tracker blocking, VPNs for traffic anonymity, and regular cookie audits. Privacy-by-design integration and consent tools ensure compliance, fostering trust and competitive advantage through transparent practices and non-invasive analytics.

Zombie Accounts

The Undead Entry Points in Your Network

Inactive or poorly managed accounts, often referred to as 'zombie accounts,' create vulnerabilities that attackers exploit as backdoors, with stolen credentials contributing to 38% of data breaches, according to Verizon's 2024 Data Breach Investigations Report.

Regular checks on user accounts help automatically disable unused ones, reducing security risks. Creating accounts only when needed limits potential threats. Stronger processes for removing access when employees or contractors leave further protect your business. These steps not only improve security but also save money, allowing you to focus on growing your business.

Ghostly Password Practices

Haunting, Lingering Vulnerabilities

Old passwords and passwords that are reused across accounts linger like ghosts and are more vulnerable to stuffing attacks. Even the 90-day change mandate often yields weak iterations, compromising security.

Shift to more secure options like biometrics or passwords supplemented by MFA. NIST-aligned passphrases enhance usability, and annual audits eliminate gaps, fortifying access controls and supporting seamless operations.

Banishing the Shadows

A Leader's Strategic Response

Cyber threats thrive in the shadows. Oftentimes, it takes a security professional to know where to find security vulnerabilities. Illumination through knowledge and action is key. Business leaders should elevate cybersecurity to board-level strategy. By addressing these risks with targeted defenses, organizations transform potential horrors into manageable challenges. Contact One Step Secure IT for expert guidance in securing your digital realm.

A One Step Secure IT eBook

Is Your IT Network a National Security Threat?

How to Elevate Your Business Above the Cybersecurity Poverty Line

Free eBook for Business Leaders

Cyber crime doesn't just threaten your profits, it jeopardizes customer trust and national security. Sophisticated hackers and ransomware gangs target businesses of all sizes, exploiting any weakness.

Our free eBook, ***Is Your IT Network a National Security Threat?***, shows you how to protect your business and America's economy.

Don't Be a Weak Link One breach can ruin your reputation or disrupt supply chains. Act now.

Discover

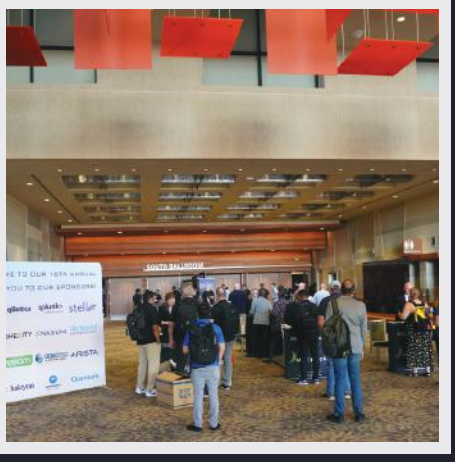
- Why cybersecurity is a business and national priority.
- Four practical steps to secure your operations.
- How AI outsmarts hackers to keep you ahead.
- Why a Managed Security Service Provider (MSSP) is your best defense.

Download Your Free eBook Today

Get actionable insights to safeguard your business, empower your team, and strengthen national security. To download your copy, scan the QR code or visit us at:

www.OneStepSecureIT.com/safeguard

Our Team Shines at the Arizona Technology Summit



The One Step Secure IT Team had a blast connecting with technology and business leaders from across the Valley at the 16th Annual Arizona Technology Summit! This conference brought together IT and security executives from all industries for a day of innovation and collaboration.

Our very own Director of IT & Security Services and CISSP, Tim Derrickson, shared his security expertise in a presentation: *Navigating the Cybersecurity Poverty Line: The Benefits and Dangers of AI.* We can't wait to return to the Arizona Technology Summit next year for more inspiring discussions and connections!

One Step rebuilds Los Angeles Business Journal's digital defenses after their...

Ransomware Nightmare

"It was a morning I'll never forget," recalls Fabian Avellaneda, Executive Assistant to the Publisher & CEO of the Los Angeles Business Journal (LABJ). On a frantic Friday in October 2022, he walked into the office to find chaos: "The internet was down, we were essentially locked out of our system."

A ransomware attack had struck the heart of LABJ, a leading voice in Greater Los Angeles business news. An unsuspecting accounting team member had clicked a malicious email link, unleashing attackers who held critical data hostage and demanded a ransom.

With the FBI and Homeland Security involved, the crisis exposed the vulnerabilities of LABJ's outdated PC-based systems and physical servers, highlighting the shortcomings of their former IT provider.

"I believe there was something our previous IT company could have done to prevent this," Fabian says, his frustration evident.

Desperate for a solution, LABJ turned to One Step Secure IT to rebuild its defenses and secure its future.

Facing the Fallout: A Call for Change

The ransomware attack was a wake-up call. LABJ's physical servers and desktops were relics, vulnerable to modern threats.

Their previous provider had "dropped the ball," as Fabian puts it, failing to implement robust defenses. They sought a managed service provider with significant expertise in cybersecurity.

Referred by their cyber liability insurance provider, LABJ partnered with One Step Secure IT. The goal was clear: modernize LABJ's infrastructure, migrate to a secure Apple environment, and exceed their insurance provider's standards with industry best practices.

Crafting a Secure Future: One Step's Solution

Beginning in spring 2023, One Step led a careful migration to a more secure IT network, evaluating LABJ's needs and implementing tools to boost both efficiency and security. The partnership transformed LABJ's operations. Their strategy included:

Transition to Apple and Cloud

One Step replaced outdated PCs and servers with MacBooks and a cloud-based infrastructure, eliminating vulnerabilities and improving scalability.

"The silver lining of the attack is that it forced us to modernize," Fabian notes. "With the assistance of One Step, we were able to get all of our staff members on MacBooks. We are now on the cloud, which is also more secure."

Fortified Cybersecurity

With CISSP-certified experts, One Step implemented robust protections, including simulated phishing attacks and training, emphasizing the importance of ongoing vigilance.

Dedicated Support

LABJ works with a dedicated network administrator, Peyton Hitchcock, who is familiar with their technology and maintains smooth and secure operations.

"As office manager, I often input a lot of tickets on behalf of the company," Fabian says. "Peyton is always very responsive and helpful when we need him."

Proactive Collaboration

Regular meetings with One Step's leadership, including Tim Derrickson, ensured transparency in their partnership.

"Tim will have meetings, once every quarter, if not more, with my publisher and myself just to go over the state of things," Fabian says, appreciating the communication.

A New Era: Security and Confidence Restored

"With One Step's help, I do feel better in regards to security," Fabian shares. "I've learned a few things from Peyton along the way."

Streamlined Workflows

MacBooks and cloud access empowered staff to work efficiently anywhere, modernizing LABJ's operations.

Proactive Partnership

Quarterly Security Briefings with One Step's team address ticket trends and potential issues. "That communication is something we didn't necessarily always have with our old company," Fabian notes.

Empowered Staff

The attack left LABJ shaken and uneasy, but One Step's training has fostered a culture of vigilance. "We're all constantly thinking about cybersecurity. 'That email doesn't look right' or 'I'm going to pick up the phone to make sure this is legitimate,'" Fabian explains.

Building Resilience: A Lasting Partnership

The ransomware attack could have been LABJ's undoing, but One Step Secure IT transformed it into a turning point. By guiding LABJ to a secure, cloud-based Apple system, they rebuilt trust and operational strength.

"Our experience has been very positive," Fabian reflects, his confidence in LABJ's digital future restored. With One Step Secure IT as their partner, LABJ now stands stronger with a fortified IT foundation and a vigilant team.

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