SYSTEMSEVEN

RESCUING A TEXAS MEDICAL PRACTICE FROM RANSOMWARE

A Critical Call for Help

In 2022, a medical practice with four locations in Texas faced a ransomware attack that targeted their QuickBooks server. With no backups in place, the situation quickly escalated. That's when they reached out to us for help. We stepped in, guided them through the aftermath, and secured both their data and their business.

What Happened?

The attack seemed to come out of nowhere. Their server was compromised through a phishing email, and by the time they realized, it was too late—they were locked out of QuickBooks and hit with a ransom demand.

The impact? It was tough. They ended up paying over $100,000 to the attackers, plus additional IT Forensics costs, much of which wasn't covered by their cyber insurance. Operations were down for days, with accounting and billing disrupted for weeks. The total financial damage reached into the hundreds of thousands.

Our Response

When they called us, they'd been struggling to get help for weeks. SYSTEMSEVEN stepped in, not just for a quick fix—we stayed until the job was done. We migrated everything to secure, cloud-based servers, wiped and re-imaged all their machines, and rebuilt their network with proper security.

Working with their leadership and forensics team, we quickly put a plan in place. The entire project—migration, reimaging, and network overhaul—took about a month, and the relief was immediate.

SYSTEMSEVEN

TRANSFORMING SECURITY AND PEACE OF MIND

After completing the project, the transformation was remarkable. Their servers were secure and backed up, and passwords were now fortified like Fort Knox. We implemented multi-factor authentication (MFA) for the entire team and ensured their emails were monitored 24/7, focusing on long-term safety.

The leadership felt immense relief and gratitude, even leaving us glowing reviews. It was a significant turnaround.

The Cost of Not Being Proactive

In hindsight, the breach had a major financial impact, causing halted production, a frozen billing department, and significant revenue loss. Despite the challenges, our swift response secured their systems, protected patient relationships, and kept the damage largely behind the scenes, avoiding blacklisting.

What We Learned

Our advice: Don't wait for disaster to assess your IT. Many clients aren't sure their data is secure or backed up, and IT providers often overlook best practices.

Future-Proofing Their Security

Our proactive approach focuses on prevention, not just problem-solving. Here's how we keep this client safe:

- Automated anti-phishing and anti-ransomware tools monitor their systems.
- MFA on all devices and servers ensures secure access.
- Centrally managed password tools simplify and strengthen security.
- Regular risk assessments and on-site visits provide peace of mind.

Download this checklist and start securing your business today. Let's avoid that "what now?" moment.

DOWNLOAD

The **SYSTEM**SEVEN Difference - Tools That Matter

Protecting them meant building a comprehensive security shield. We implemented:

- MS365 tools to secure email.
- MFA to tighten access.
- Centralized password management for simplicity and security.
- Security Awareness Training to address the human factor.
- Backup and Disaster Recovery Planning to prevent future nightmares.

At the end of the day, we're more than their IT provider—we're their partner, protector, and a bit of their superhero. They trust us not just for fixing what others couldn't but for standing by them to ensure it never happens again.