LeadingIT

December 2025

The NetWork

- THE SILENT BREACH: WHAT 5.6 MILLION YALE NEW HAVEN HEALTH PATIENTS CAN TEACH CHICAGO BUSINESSES ABOUT CYBERSECURITY
- WHEN RANSOMWARE LEARNED TO WRITE ITSELF
- WHY SKIPPING SOFTWARE UPDATES IS RISKIER THAN YOU THINK

On Cover: Laura, Christa, Kelly, Orlando

The Silent Breach: What 5.6 Million Yale New Haven Health Patients Can Teach Chicago Businesses About Cybersecurity

On March 8, 2025, Yale New Haven Health discovered hackers had quietly infiltrated their network and stolen data from 5.6 million patients. What made this breach alarming wasn't just its scale—it was how silently it happened.

This wasn't a typical ransomware attack. No group claimed responsibility, no dark web posts appeared. The hackers simply slipped in, copied sensitive data, and disappeared, exfiltrating patient names, dates of birth, Social Security numbers, and medical record numbers.

According to the HIPAA Journal's 2024 Healthcare Data Breach Report, this breach represents just one of 725 large healthcare breaches reported last year. On average, 758,288 healthcare records were compromised every single day in 2024.

What Actually Happened at Yale New Haven Health

Yale New Haven Health operates Connecticut's largest healthcare system with five hospitals, 360 outpatient locations, and 30,000 health professionals.

March 8, 2025: IT teams detected unusual activity and immediately contained the threat, launching a formal investigation. Three days later, the health system publicly announced the incident. After forensic analysis by Mandiant, Yale confirmed by April 11 that an unauthorized third party had exfiltrated patient data. By April 14, notification letters began reaching affected patients.

The electronic medical record system remained operational throughout. Hackers accessed administrative data—names, contact information, demographic details—but not clinical treatment records or financial information. Still, exposing 5.6 million individuals' personal data triggered immediate class action lawsuits and federal investigations.
Most concerning: no ransomware group claimed responsibility, suggesting sophisticated criminal operations.

The Vulnerabilities That Enable Silent Intrusions

According to the HIPAA Journal, hacking and IT incidents now dominate breach reports—a massive shift from lost laptops and misfiled paperwork.

Modern breaches succeed because attackers exploit gaps in continuous monitoring, moving laterally through networks while escalating privileges slowly to avoid detection.

Common vulnerabilities include:

- Unmonitored network segments where unusual activity goes unnoticed
- Delayed patch management that leaves known vulnerabilities exposed
- Insufficient access controls allowing lateral movement once initial entry is gained
- Incomplete asset inventories creating blind spots in coverage
- Lack of behavioral analysis to detect unusual login patterns

The challenge facing Chicago businesses: detecting the anomaly before data leaves your network.

Cont. – The Silent Breach: What 5.6 Million Yale New Haven Health Patients Can Teach Chicago Businesses About Cybersecurity

What Proactive Security Actually Looks Like

Reactive organizations discover problems after damage is done. Proactive organizations identify threats in progress and stop them.

Effective protection requires layered defenses:

24/7 network monitoring provides real-time visibility. When behavioral patterns shift—unusual login times, unexpected data access, abnormal file transfers—alerts trigger immediate investigation.

R**apid response protocols** mean incidents get contained within minutes, not days. The faster the response, the less data leaves your network.

Regular vulnerability assessments identify security gaps before attackers exploit them.

Network segmentation limits damage if breach occurs. Attackers can't simply move from one compromised area to your entire infrastructure.

Multi-factor authentication blocks unauthorized access even when credentials are compromised. The absence of MFA has been cited in numerous major breaches, including the catastrophic Change Healthcare attack that, according to the HHS Office for Civil Rights, affected 190 million people.

Continuous compliance monitoring ensures HIPAA, FTC, and PCI standards remain in place as systems evolve.
Organizations working with managed cybersecurity solutions benefit from these capabilities operating continuously without requiring extensive internal security teams.

Lessons for Chicagoland Organizations

Healthcare organizations aren't the only targets. Any business managing sensitive information faces similar threats:

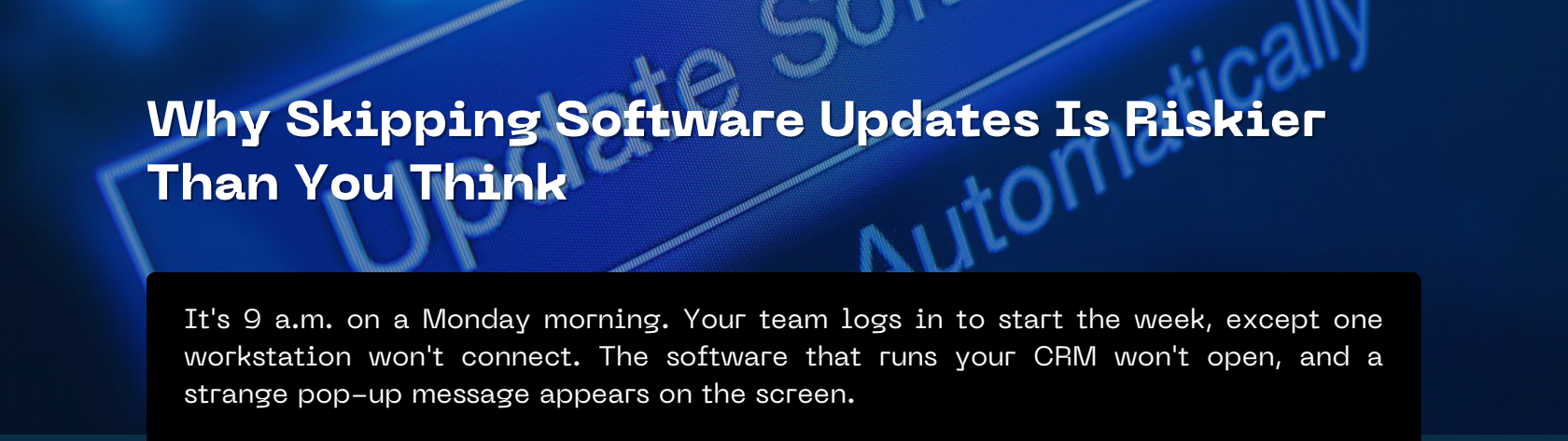
- CPAs handling sensitive financial records
- Law firms protecting privileged client communications
- Private schools maintaining student and family data
- Nonprofits storing donor information

Chicago SMBs face greater risk because they often lack security resources of larger organizations while possessing valuable data. The lesson isn't about implementing every security tool available—it's about having continuous expert oversight, immediate threat detection, and rapid response capabilities.

Moving Forward

The Yale New Haven Health breach reminds us that even well-resourced organizations with dedicated IT teams can experience sophisticated attacks. What matters most is having continuous monitoring, expert analysis, and rapid response capabilities working together.

For organizations handling sensitive data, the question isn't whether you'll face cyber threats—it's whether you'll detect them quickly enough to prevent serious damage.



Why Skipping Software Updates Is Riskier Than You Think

It's 9 a.m. on a Monday morning. Your team logs in to start the week, except one workstation won't connect. The software that runs your CRM won't open, and a strange pop-up message appears on the screen.

The culprit? A missed update from three months ago. That tiny patch was meant to fix a known vulnerability, but it was never installed. Now your system is down, your employees are stuck, and your IT team is scrambling to recover.

For many businesses, skipping software updates feels harmless, an "I'll get to it later" task that always gets pushed back. But in today's threat landscape, an outdated system isn't just slow or inconvenient. It's a welcome mat for cybercriminals.

The Hidden Costs of Ignoring Updates

Every piece of software, from your operating system to your email client, has potential weak spots. When developers find those vulnerabilities, they release updates to fix them. But when updates are ignored, those vulnerabilities remain wide open—and hackers know exactly how to find them.

Unpatched systems represent a significant and growing threat to businesses. According to Verizon's 2024 Data Breach Investigations Report, vulnerability exploitation nearly tripled in just one year, now accounting for 14% of all confirmed breaches and that percentage continues to climb.

The surge is even more dramatic when you look at the numbers: attacks exploiting unpatched vulnerabilities surged 180% year-over-year, driven primarily by ransomware actors targeting systems that haven't applied critical updates. These aren't zero-day exploits or sophisticated, state-sponsored hacks. They're attacks that could have been prevented with a simple update.

Beyond the obvious security risks, running outdated software affects performance and reliability. Systems slow down, integrations break, and downtime increases. That downtime adds up fast, lost productivity, frustrated employees, and potential damage to your reputation with clients.

And let's not forget compliance. Many cyber insurance policies and IT compliance services now require proof of regular patch management. Falling behind on updates could mean more than just a security risk, it could mean losing coverage when you need it most.

The message is clear: delaying updates isn't just inconvenient—it's dangerous.

What "Regular Updating" Really Means

When most people think of software updates, they picture the occasional Windows restart. But according to the Verizon DBIR, it takes organizations an average of 55 days to patch 50% of critical vulnerabilities—plenty of time for attackers to exploit them.

A complete patching strategy includes:

- Operating system updates that protect against the latest threats
- Third-party software patches for applications like Office, Adobe, and CRM tools
- Firmware updates for routers, firewalls, and network switches
- Security tool updates for antivirus, EDR, and browser protections

The goal isn't just to install updates, but to do so strategically, testing and deploying them in a way that protects uptime and stability. That's why businesses partner with managed IT services providers: to take the guesswork out of when and how to update.

Proper patch management is about being proactive, not reactive. Instead of waiting for something to break or for an exploit to be discovered, the process runs quietly in the background, keeping systems protected around the clock.

The Business Benefits of Staying Updated

When your systems are always up to date, your business runs better, plain and simple:

- Security you can trust – Every patch closes a door that hackers might try to pry open
- Better performance – Updates improve system stability, reduce bugs, and boost compatibility with new software
- Fewer disruptions – Preventing a crash or breach is far less expensive (and stressful) than fixing one
- Compliance peace of mind – Consistent patching keeps your company aligned with data protection standards like HIPAA, PCI, and NIST
-

The real benefit, though, is confidence. You can focus on growth and serving clients, knowing your systems are quietly doing their part in the background, secure, stable, and always current through proactive IT management.

When Ransomware Learned to Write Itself

In late 2025, a mid-sized manufacturing firm woke to critical production servers frozen by ransomware, extortion notes on operator consoles, and evidence of data theft. The ransom demand was unusually large, and the malware was oddly targeted, fighting every automated detection and adapting to defensive actions in near-real time.

Investigators concluded this was not the work of yesterday's code-script kiddies. The attacker used AI tooling to design polymorphic payloads, craft lateral-movement strategies, and automatically re-deliver payloads when defenses threw up obstacles.

In short: the attackers were using artificial intelligence to be faster, smaller, and smarter than the defenses the company relied on.

This is AI-generated ransomware in action. It accelerates and automates existing threats. What used to require a skilled programmer and long testing cycles can now be iterated in hours. Phishing lures are hyper-personalized by generative models. Malware samples mutate automatically to evade signature detection. Extortion negotiations are run through chatbots that scale attacks across many victims simultaneously.

The Data Tells a Concerning Story

- Research shows that adversarial malware generators can increase evasion rates by 15.9% against top antivirus tools, making AI-enhanced malware increasingly difficult to detect
- 48% of organizations cite AI-automated attack chains as the greatest ransomware threat today, with 85% believing legacy defenses are becoming obsolete
- The average total cost of a ransomware incident now reaches $5.5-6 million, including ransom payments, business disruption, and recovery
- Between September 2024 and February 2025, phishing campaigns saw a 22.6% increase in ransomware payloads, with 82.6% of all phishing emails exhibiting AI usage

The result is a dangerous multiplication of risk. Where a single attack once required significant effort and time, AI lowers those costs and multiplies opportunities. That means more incidents, faster escalation, and higher likelihood of significant data exfiltration and operational downtime.

Cont. – When Ransomware Learned to Write Itself

What Business Leaders Can Do

At LeadingIT we treat this as both a technical and organizational problem, and we design responses accordingly:

Continuous Behavioral Detection

AI-generated threats avoid old signatures, so we focus on anomalies: unusual process behavior, spikes in data traffic, lateral logins that don't match user history. Our security operations center ingests telemetry from endpoints, network sensors, and identity systems to correlate signals that individually look benign but together tell a story.

Instant Automated Containment

We use micro-segmentation to limit lateral movement and enforce least-privilege so stolen credentials cannot open every door. Critical systems are isolated into hardened zones, and automated playbooks revoke access and quarantine affected hosts the moment an incident is suspected.

Resilience Over Reliance

Immutable, air-gapped backups and tested recovery processes mean ransom by deletion or encryption becomes far less effective. When recovery is fast and predictable, attackers lose leverage. We conduct realistic tabletop and red-team exercises so people know how to act, who to call, and what to prioritize when chaos hits.

Human Risk Management

Because AI can craft extraordinarily convincing social-engineering, including deepfakes and voice-spoofing, ongoing phishing simulations, role-specific awareness training, and multi-factor authentication are non-negotiable. We help clients harden identity, manage third-party access, and rotate machine-identities so attackers cannot repurpose service accounts.

The Difference Preparation Makes

The manufacturing firm ultimately recovered after decisive containment and a staged restore from clean backups, but the episode cost weeks of production and significant customer confidence. It avoided paying ransom because its recovery strategy worked. That outcome is the difference between a news headline and an internal post-mortem. AI is changing the pace and scale of ransomware, but not the fundamental defensive posture that keeps organizations safe. Vigilant monitoring, rapid containment, tested recovery, and a people-first security culture blunt the advantage attackers hope to gain from automation.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

SCAN TO LEARN MORE

815-788-6041 GOLEADINGIT.COM/REFER

DRIVEN – CHASES EXCELLENCE – HUMBLY CONFIDENT – ACCOUNTABLE – STAYS POSITIVE

LeadingIT Core Values Victor of the Month

Congratulations to Dustin, our Values Victor this month for Accountability!

As someone who consistently leads by example, Dustin takes ownership of his work and holds himself to a high standard, both for our clients and within the team. He understands that accountability isn't just about tracking numbers (though we do that, too); it's about owning outcomes, learning from challenges, and always making IT right.

Well deserved, Dustin!

LeadingIT

We Help Chicagoland Organizations Eliminate Concerns Over IT and Cybersecurity Where the Unsolvable is Solved with Unlimited Support, and an Unbeatable Guarantee.

WE ARE CELEBRATING!

BIRTHDAYS

CHRISTA GIBBONS 12/14

ANNIVERSARIES

ALEX DEL FIACCO 2 YEARS