LeadingIT

August 2025

The NetWork

- WHY CYBERCRIMINALS ARE SAVING YOUR DATA FOR LATER
- 5 IT MISTAKES MANUFACTURING BUSINESSES CAN'T AFFORD TO MAKE
- THE QUIET THREAT INSIDE YOUR BUSINESS: OFFBOARDING GAPS
- PROTECTING DONOR AND TUITION DATA: IT SECURITY TIPS FOR PRIVATE SCHOOLS

Quarterly Update — July 2025

A Note from Stephen & Laura
(Your V/I Duo)

Hey there,

At LeadingIT, we believe in doing IT right—100% of the time—and that starts with how we run our business behind the scenes.

Every 90 days, we step out of the day-to-day to refocus and re-align using the Entrepreneurial Operating System (EOS), a powerful framework that keeps our team accountable, our goals clear, and our momentum strong.

We've got a solid Visionary/Integrator rhythm fueling this machine: Stephen (our Visionary) brings the energy, creativity, and forward-thinking vision, while Laura (our Integrator) turns those ideas into reality—making sure people, processes, and priorities stay on track. It's that balance that drives everything we do.

We just wrapped up another powerful quarter, hitting 100% of our company-wide Rocks (our most important goals), and we're excited to give you a peek behind the curtain:

What We Knocked Out in Q2:

- Even faster onboarding. Our Instant Onboarding process is now more streamlined for a quicker, smoother kickoff.
- A stronger first 100 days. We mapped out your full journey to ensure a consistent, high-touch experience from day one.
- Happier team, better service. Our employee eNPS hit 95%! Happy techs = better support. (And let's just say there was a time when it was in the negatives).
- Launched our Unbeatable Guarantee. Try us risk-free for 60 days—if your team doesn't love us, we work for free. Plus, we price match.
- Enhanced our prospect experience. Our sales process is now faster, more transparent, and more educational for those exploring IT support.
- Invested in LeadingIT University. Our internal training program now includes advanced leadership and customer service tracks, so our team continues to grow alongside your needs.
- We proactively prepared -and still are preparing- clients for upcoming Microsoft changes, including Windows 10 support ending this October and end-of-life announcements for older versions of Windows Server.

What's On Deck for Q3:

Here's where we're focusing our energy this quarter to keep improving your experience:

- Improving how we use automation to reduce ticket volume and resolve recurring issues more efficiently.
- Providing advanced training for our technical teams on cybersecurity, compliance, and new tools.
- Strengthening our account management check-ins so we stay connected with your business needs.
- Greater financial clarity. We're giving department heads more visibility into the numbers so they can make faster, better decisions.

All of this ties back to our EOS mindset, clear goals, empowered leaders, and continuous improvement every quarter.

Interested in EOS for Your Own Business?

If you're curious about how EOS could help you lead with more clarity and less chaos, we'd love to share what it's done for us. Reach out to either one of us, (Stephen or Laura) we're always happy to chat about how EOS might fit your leadership journey too.

Thanks for being part of ours.
Here's to what's next!

Stephen & Laura
Visionary & Integrator
Team LeadingIT

Why Cybercriminals Are Saving Your Data for Later

Imagine someone breaking into your house, stealing a safe they can't open yet, and planning to crack it in a few years when they get better tools. That's exactly what cybercriminals are doing with your data today.

This method is called "harvest now, decrypt later." Hackers are stealing encrypted files now, knowing that powerful computers in the future will eventually be able to unlock them. The scary part? Your sensitive data could already be sitting in a hacker's storage, just waiting for the right time.

What Are They Saving?

They're after emails, donation records, financial data, medical info, and anything else that could be valuable, either now or years from now. Even if your data is encrypted today, it may not stay protected in the future if quantum computers become strong enough to break current security standards.

According to experts, this is not science fiction. Countries and cybercrime groups are already collecting encrypted data for future use. The U.S. government has started preparing for this very threat because quantum computers could be widely available by the 2030s.

Why Should You Care Now?

It's easy to think, "We'll handle it when the time comes." But if hackers steal your encrypted data today, it may be too late to protect it tomorrow.

For example:

- A donor list or financial record you thought was safe might be leaked years from now.
- Student or employee data could be exposed long after someone has left your organization.
- You might face fines or lawsuits if private data becomes public, even years after it was stolen.

What You Can Do Today

Here are simple steps you can take now to protect your data:

1. Tell your IT provider to start planning for quantum security. There are new types of encryption designed to stay strong even in a world with quantum computers.
2. Use flexible systems. Make sure your systems can upgrade to new security tools as they become available.
3. Protect your most important data first. Not all data is equal, start with financial records, donor information, and personal details.
4. Back up data securely. Store backups in places that use strong encryption and modern protection.

We Help You Stay One Step Ahead

You don't need to be a tech expert to take this threat seriously. At LeadingIT, we've helped Chicago-area organizations protect their data for years. We stay ahead of emerging threats and help schools, nonprofits, and businesses do the same, so your information stays protected both now and in the future.

5 IT Mistakes Manufacturing Businesses Can't Afford to Make

In manufacturing, downtime isn't just annoying—it's expensive. One hour of halted production can cost thousands, delay shipments, and damage customer relationships. And too often, it's not a machine that fails, it's the IT behind it.

Here are five IT mistakes manufacturers can't afford to make and how to avoid them.

1. No Backup or Disaster Recovery Plan

If your systems go down due to ransomware, server failure, or a natural disaster, how quickly could you bounce back? If your answer is, "I'm not sure," that's a big risk.

Manufacturers need reliable backups and a tested disaster recovery plan. According to IBM's Cost of a Data Breach Report, the average recovery cost is over $4 million, and that includes operational downtime. Don't let your floor go quiet while your data scrambles to recover.

2. Running Outdated Software on Critical Systems

Old software isn't just slow, it's vulnerable. When ERP systems, SCADA platforms, or even accounting tools go unpatched, they become easy targets for hackers.
Keep your systems current with regular updates and patch management. A single unpatched flaw can open the door to cybercriminals looking to shut down operations or steal valuable production data.

3. Weak Network Security in Connected Environments

Today's manufacturing tech is more connected than ever. IoT sensors, remote monitoring, cloud platforms, and mobile apps offer real advantages. But with that convenience comes risk.

Without proper network segmentation, firewalls, and endpoint protection, a single compromised device can spread malware across your entire environment. The Cybersecurity and Infrastructure Security Agency (CISA) recommends segmenting networks and implementing zero trust strategies to reduce exposure.

4. No Real-Time IT Monitoring

Downtime rarely gives warning. But with 24/7 monitoring, small issues can be spotted before they snowball.
A Managed IT provider can track system health, flag errors, and even resolve problems remotely before your line grinds to a halt. It's the difference between being proactive and being blindsided.

5. Neglecting User Training and Access Controls

Most cyberattacks start with a simple mistake like an employee clicking a fake email or using a weak password.

Make cybersecurity part of your safety culture. Train your team, enforce strong login policies, and limit system access based on job roles. These steps cost very little but make a huge impact.

Don't Let IT Slow Down Your Production Line

Manufacturing success depends on uptime, precision, and reliability. Your IT should match that standard. Avoiding these five mistakes can save you from costly outages and give you peace of mind that your operations are secure.

The Quiet Threat Inside Your Business: Offboarding Gaps

When we talk about cybersecurity, most people picture firewalls, phishing emails, or ransomware. But one of the most overlooked threats to your organization is much quieter: former employees who still have access to your systems.

The Risk You Can't See

The danger of poor offboarding is not just theoretical, it's measurable. In a recent study, 56% of respondents admitted to using their continued digital access to actively harm a former employer, and 24% said they intentionally kept a password after leaving the company. That means nearly one in four former employees are walking out the door with keys to your network, and more than half are willing to use them.

Whether it involves accessing client data, deleting files, or disrupting operations, these actions can lead to serious financial and legal consequences. Without a strict offboarding process, your business may never see the next threat coming.

Real-World Fallout

This is not a hypothetical risk. A recent study by OneLogin revealed that 20% of organizations have experienced data breaches caused by former employees. Whether it is due to revenge, negligence, or simple oversight, these gaps can lead to compliance violations, data leaks, or serious business disruptions.

Why It's So Common

Manual offboarding processes are time-consuming and error prone. According to TechRepublic, 32% of former employees retain access for more than a week after departure, and 20% for more than a month. In many cases, no one owns the complete offboarding checklist across departments, and IT only learns about a departure after it is too late.

How to Close the Gaps

- Inform your IT service provider immediately. As soon as an employee is terminated or resigns, notify your IT team so they can promptly disable all user accounts, revoke access to sensitive data, and recover company-owned devices.
- Centralize and automate access management. Work with your provider to implement identity and access management (IAM) tools that streamline offboarding and reduce the chance of oversight.
- Create a documented checklist. Make sure HR, IT, and department managers follow a consistent, end-to-end process every time.
- Audit regularly. Perform quarterly access reviews to identify unused or orphaned accounts.

Make Security Part of the Exit Process

A secure offboarding process is not just about protecting your data. It is about protecting your people, your clients, and your reputation. The sooner you address these access risks, the safer your organization will be.

Protecting Donor and Tuition Data: IT Security Tips for Private Schools

Private schools manage highly sensitive information, from donation records and tuition payments to student and family details. A breach can damage trust, disrupt operations, and even lead to legal consequences. Here are essential IT security strategies to safeguard donor and tuition data.

Understanding the Stakes

Recent trends show fundraising success now depends heavily on data privacy. As one report notes, "donors are going to require nonprofits they support to safeguard their information" and 11 U.S. states have enacted comprehensive data privacy laws that include nonprofits as of late 2024 (source).

Meanwhile, financial aid and tuition platforms carry deeply personal data—bank account numbers, Social Security numbers, tax returns, and student records. If this data is mishandled it can lead to identity theft and compliance violations.

High-Impact Security Measures

1. Encrypt Data at Rest and in Transit

Choose systems that support encryption, ensuring that both stored and transferred donor and tuition data remains protected—even if systems are compromised.

2. Enable Secure Authentication

Require multi-factor authentication (MFA) for access to donor management systems, tuition portals, and financial aid platforms. MFA greatly reduces the risk of unauthorized access.

3. Restrict Access by Role

Use role-based access controls to limit who can view or modify donor and tuition records. This reduces insider risk and ensures users only access what they need.

Protecting Donor and Tuition Data: IT Security Tips for Private Schools

4. Train Staff and Volunteers

Regular cybersecurity training helps everyone recognize phishing, social engineering, and safe data handling practices. Ensure anyone with financial or personal data access knows about secure sharing methods and device policies.

5. Regularly Audit and Review

Conduct quarterly access audits to verify only authorized personnel have access. Remove permissions immediately when roles end or staff leave the organization.

6. Keep Systems and Backups Current

Install updates and patches promptly. Maintain secure, offline backups of all critical financial and donor data to ensure recovery from ransomware attacks or system failures.

Building a Culture of Privacy

Educating staff, families, and even alumni about data privacy strengthens institutional trust. Share your commitment to protecting donor and tuition information and encourage best practices for creating strong passwords, enabling MFA, and reporting issues. Transparency builds confidence.

Protecting What Matters Most

Securing donor and tuition data is not just a technical issue. It is central to your school's credibility and long-term success. The right IT infrastructure, clear processes, and a culture of security awareness all play a role in keeping your community safe.

$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!**

815-788-6041 **GOLEADINGIT.COM/REFER**

SCAN TO LEARN MORE

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

LeadingIT Core Values Victor of the Month

Mallory Rocha - Congratulations to this month's Values Victor for staying positive!

Mallory was chosen for consistently embodying one of our favorite core values: Staying Positive. In the fast-paced world of IT, challenges are inevitable, but Mallory meets them all with a smile, a can-do attitude, and a laser focus on finding solutions.

Whether it's tackling daily office operations, HR tasks, billing or jumping in to support a teammate, Mallory leads with optimism and a solution-first mindset.

Thank you for the energy, encouragement, and excellence you bring to the team. We're lucky to have you!

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

STEPHEN TAYLOR	8/11
MAX KULWIEC	8/24
MALLORY ROCHA	8/30

ANNIVERSARIES

MIKE TARASIEWICZ	2 YEARS