LeadingIT

November 2025

The NetWork

- LEADINGIT QUARTERLY UPDATE
- HOW TO MANAGE BACKUP AND DATA RECOVERY FOR CHICAGO BUSINESSES
- STILL REUSING PASSWORDS? HERE'S WHY THAT'S RISKY (AND WHAT TO DO ABOUT IT)

On Cover: Jeremiah, Orlando, Stephen, Laura, Imran, Izaac, and Seth

A Note from Laura Piekos, President

New Roles, Big Goals, and a Few Google Reviews Along the Way

As we move into Q4, I'd describe the last quarter as a mix of successes, a few losses, and a whole lot of figuring IT out. We learned, we adjusted, and we came out stronger. That's what growth looks like, and as we celebrate 15 years of LeadingIT, I couldn't be prouder of the direction we're headed together.

Q3 Highlights

This quarter we focused on getting the Right People in the Right Seats. We welcomed a new Service Delivery Manager whose mission is to make sure every client gets service they truly love and want to share about. (No pressure Izaac!)

We also celebrated some amazing internal growth. Kelly stepped into her new role as Director of Business Development, moving from setting appointments to taking them. She's off to an incredible start, and it's exciting to see her thrive in this next chapter.

Celebrating 15 Years

October marked 15 years of LeadingIT. Fifteen years ago, Stephen took a leap and turned his side gig into something more by creating LeadingIT, a company he knew could do IT better. I was busy teaching toddlers at the YMCA and working toward a degree in social work. It wasn't exactly an obvious path to running an IT company, but that's the beauty of finding people who share your values and vision. When you surround yourself with the right team, doors open that you never expected, and the journey becomes something bigger than you imagined.

What amazes me most isn't just how much has changed in 15 years, but how much has stayed the same. We're still driven by that same energy, curiosity, and drive to do things better. And now, everyone here knows where we're going for the next 15 years, and more importantly, how they're helping us get there. The road ahead feels limitless when everyone's heading in the same direction.

A Note from Laura Piekos, President

New Roles, Big Goals, and a Few Google Reviews Along the Way

Giving Back

This quarter's Google Review Competition was a huge hit. Every time a technician was mentioned in a review, we treated them to lunch, and for every review received, we donated to a local nonprofit. This round's focus was NAMI McHenry County, and through reviews and fundraising, our team and clients helped make a donation of more than $4,000 to support local mental health programs (over $1,550 of that came directly from clients being awesome enough to leave us a Google review).
We love giving back, and as we continue to grow, we're always looking for more ways to share our time, talent, and resources with our community.

Looking Ahead

As we move into Q4, we're keeping our focus where it belongs, on our people, our clients, and continuous improvement. We're investing in staff development, building more automation, and streamlining the behind-the-scenes work so our clients continue to feel the difference through faster service, better communication, and smoother experiences.

Fifteen years in, we're still learning, still evolving, and still doing what we love. Thank you for being part of the journey and for helping us build something that keeps getting better every year.

– Laura Piekos, President

How to Manage Backup and Data Recovery for Chicago Businesses

According to Nationwide Insurance, nearly three out of four small businesses lack a data recovery plan. In the Chicago area, that risk is amplified by two threats: an evolving cyber landscape and unpredictable Midwest weather that brings an average of 54 tornadoes a year. A well-structured data backup and recovery plan can protect against both digital attacks and physical disasters.

Start With the 3-2-1-1-0 Rule

The foundation of strong backup management is the 3-2-1-1-0 strategy: three copies of your data, on two different storage types, with one copy stored away from your office, one backup that cannot be changed or deleted, and zero errors verified through regular testing.

This layered approach protects against multiple threats:

- Local backups enable fast recovery from routine incidents
- Cloud storage provides geographic redundancy against Chicago's flooding and power outages
- Immutable backups defend against ransomware targeting backup repositories

When these layers work together, businesses achieve stronger redundancy and faster recovery times. Professional IT teams can automate the process, ensuring every backup runs consistently without requiring daily oversight.

Set Your Recovery Goals

Every business must define how quickly systems should be restored and how much data loss is acceptable during a disruption. These measures are known as Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Not every system is equally critical. For example:

- Payment processing: Must be back up immediately with no data loss
- Email systems: Can be down for hours, losing a few minutes of emails is acceptable
- Document storage: Can be down for days, losing a few hours of work is manageable
-

Start by prioritizing your most critical systems. Identify which applications drive revenue or contain irreplaceable data. Partnering with a virtual CIO helps align recovery goals with your overall business strategy so resources are invested where they matter most.

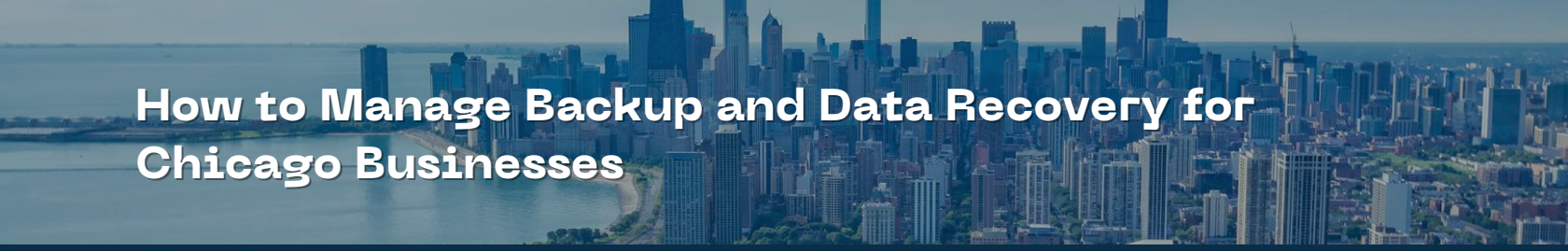
Set Up Automatic Backups

Manual backup processes often fail simply because someone forgets to run them. Automated systems eliminate that risk by performing scheduled backups reliably and consistently.

Automation should include:

- Scheduled daily backups
- Continuous copying for critical systems
- Monitoring with automatic alerts
- Encryption during storage and transfer
- Retention of 30-90 days of backup versions

Professional monitoring ensures backups complete successfully and that data remains intact. Many businesses only discover failures when it is too late—during a real disaster. With the right setup, backup traffic flows efficiently, ensuring every file is ready when needed.



How to Manage Backup and Data Recovery for Chicago Businesses

Test Your Recovery Systems Regularly

Testing is the most overlooked part of backup planning. Even the best systems are only valuable if they actually work when disaster strikes.

According to Gartner, 76% of companies experienced an incident in the past two years that required their disaster recovery plan, with more than half facing multiple incidents. Despite this frequency, many never verify that their systems work until disaster hits.

Test critical systems every three months and all others at least twice per year. Testing also trains your staff on procedures and identifies outdated instructions. Chicago-area businesses should also test scenarios unique to the region. For example, can operations continue during multi-day power outages or severe storms? Can remote employees access systems if local connectivity fails?

Follow Industry Rules

Compliance is another essential part of recovery planning. Industries like healthcare and finance face additional requirements that go beyond standard IT policies.

Healthcare companies must follow HIPAA Security Rule requirements, including regular testing of data recovery plans. Businesses that process credit card payments must meet PCI DSS standards, and the FTC Safeguards Rule requires written response plans that include recovery procedures and encryption protocols.

Partnering with experts in IT compliance services ensures your backup strategy meets both regulatory and business continuity goals.

Build a Complete Recovery Plan

A successful recovery plan brings everything together. It should be written, tested, and easily accessible. Include step-by-step recovery actions, system dependencies, vendor contacts, and communication details for internal and external teams.

Assign clear roles in your recovery team, including:

- Executive sponsor
- Recovery coordinator
- Technical team members
- Communication specialists
- Network or infrastructure experts

Communication plans should cover both internal updates and external messaging across multiple channels.

Still Reusing Passwords? Here's Why That's Risky (And What to Do About It)

When most businesses think about cybersecurity, they imagine firewalls, antivirus software, or hackers trying to crack complicated codes.

But one of the biggest cybersecurity threats is much simpler: weak passwords.

According to the Verizon Data Breach Investigations Report, more than 50% of data breaches involve stolen or reused credentials. And for businesses across Chicagoland, especially in healthcare, finance, legal, and nonprofit sectors, that's a major risk.

Why Passwords Still Matter (A Lot)

Think of passwords as the keys to your business. If they're weak, predictable, or shared among team members, a cybercriminal doesn't need fancy tools—they just log in.

Microsoft's Digital Defense Report found that 97% of identity attacks target passwords. Let that sink in.

Here are a few common password pitfalls we see all the time:

- Reusing passwords across different platforms
- Using defaults or simple options like "Welcome123"
- Skipping multi-factor authentication (MFA)
- Sharing logins across employees without any safeguards

These aren't just bad habits—they can also lead to compliance violations under laws like HIPAA, PCI-DSS, or FTC Safeguards, depending on your industry.

What a Password Manager Can Do for You

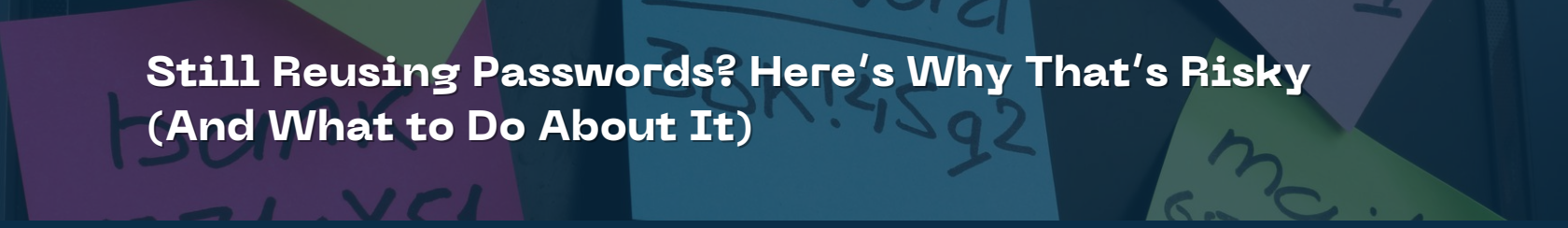
A password manager is one of the easiest and most effective tools for protecting your organization.

Instead of trying to remember dozens of logins or keeping them in a spreadsheet, a password manager creates and stores strong, unique passwords for every account. All your team needs to remember is one master password.

Some of the benefits include:

✅ Strong, random passwords for every login
✅ Less stress and fewer forgotten passwords
✅ Safer sharing between team members
✅ Alerts if one of your passwords shows up in a breach

Used properly, password managers reduce human error, still the #1 cause of cybersecurity incidents, and integrate seamlessly with multi-factor authentication and compliance tools.



Still Reusing Passwords? Here's Why That's Risky (And What to Do About It)

Common Mistakes We Still See (And Fix)

Even as awareness grows, many Chicago-area businesses still overlook password hygiene.

These are the most common issues:

- Password policies that are written but not enforced
- No MFA required for critical systems
- Employees aren't trained on phishing or login risks
- Passwords stored in spreadsheets or on sticky notes
- Compliance gaps that leave your organization exposed

The truth is, password security isn't just an IT problem—it's a leadership and culture issue. If leadership doesn't take it seriously, employees won't either.

The 5 Habits of Secure Companies

Good password habits don't require a huge IT overhaul, just the right tools and a little discipline.

Here's what we recommend:

1. Roll out a password manager across your organization
2. Enable multi-factor authentication on everything critical
3. Run regular password audits to find weak or reused passwords
4. Offer simple employee training to prevent phishing and credential theft
5. Align your password policies with your industry's compliance requirements

You can also work with a vCIO or IT consultant to make sure your password strategies support your long-term business goals and audit readiness.

$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

Please join us in congratulating Seth, our Values Victor for being **Humbly Confident**!

He's the kind of technician every business wishes they had, skilled, humble, and always focused on finding solutions that make a difference.

At LeadingIT, we're proud to have team members like Seth who lead with confidence and step up to get IT done!

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

GIANCARLO JABON	11/8

ANNIVERSARIES

HISSAN BADAR	1 YEAR
BRIAN DONAHUE	1 YEAR
SETH LAVIGNE	1 YEAR
LAURA PIEKOS	7 YEARS