LeadingIT

September 2025

The NetWork

The Power of an IT Vulnerability Assessment

A few months ago, we sat down with a business owner from the northwest suburbs. Mid-sized accounting firm. Sharp guy. Said to me, "We've never had a data breach, our antivirus is solid, and our backups run every night, we're good."

So we offered a risk assessment.

Guess what we found?

- *His backups were running*... but they hadn't been tested in months.
- *His Microsoft 365 accounts?* A few still had shared passwords and no MFA (multi-factor authentication).
- *Firewall?* Set up back in 2018 and hadn't been touched since.
- And no one had trained the staff on phishing emails. One click away from disaster.

Here's the truth: Most small businesses think their IT is fine, *until they see what's under the hood.*

Why a Vulnerability Assessment Matters More Than You Think

An IT vulnerability assessment isn't just a "tech checkup." It's your early warning system. It's the flashlight in the dark corner of your tech stack, showing you what you've missed.

Here's what it looks at and why each one matters:

- **Backups** – You might have them, but are they actually restoring when needed?
- **Accounts** – Who has access to what? Are former employees still hanging out in your systems?
- **Microsoft 365** – So many hidden risks here. Unsecured inboxes. File sharing wide open. Admin rights given out like candy.
- **Patches** – One unpatched system is like leaving the backdoor wide open to hackers.
- **Antivirus** – Running doesn't mean protecting. Is it current? Is it detecting? Is it alerting?
- **Firewalls** – Most were set once and forgotten. That's not defense, that's decoration.
- **Employee Education** – Your staff is your first line of defense. If they don't know how to spot a scam, you're exposed.
- **Encryption** – Sensitive data needs to be locked down, at rest and in motion.
- **Surveillance** – Not Big Brother stuff. But do you know if something weird is happening on your network at 3 a.m.?

> **"But I Have an IT Guy..."**
> Great. But who audits your IT guy?
>
> We all need a second set of eyes, especially when it comes to security. Even the best internal teams or IT vendors can miss things. A third-party assessment brings objectivity. It removes the assumptions. It validates that what you think is happening... actually is.

You Might Be Fine... But What If You're Not?

Most breaches don't start with a dramatic hack. They start with a missed update, a reused password, a sleepy staffer clicking a bad link.

A good vulnerability assessment helps you sleep better. It shines a light in every dark corner, exposes the blind spots, and gives you a clear roadmap to fix them.

It's not about selling you new tools. It's about helping you not become a cautionary tale.

The Hidden Dangers of Shadow IT

Ever had an employee come to you with a big grin, saying, “Don’t worry, I found a faster way to do it,” and then you find out they’ve been using some random app they downloaded from who-knows-where?
That, my friend, is Shadow IT.

It is when your team uses apps, devices, or cloud services without your approval or without IT even knowing about it. They might think they are being helpful, but in reality it can open the door to data leaks, compliance violations, and even cyberattacks.

Why Shadow IT Happens

Let’s be honest. Most people are not trying to cause trouble.
They are just trying to get work done faster. Maybe your accounting clerk uses a personal Dropbox to send files home, or your sales rep signs up for a free CRM to manage leads. It feels harmless in the moment.

But here is the problem:

- You do not control the security of that app.
- You do not know where the data is stored.
- You do not know who else can access it.

It is like letting someone store your client files in a random storage unit without checking the locks.

The Real Risks Behind Shadow IT

For a small business owner, the dangers are not just “tech problems.” They hit where it hurts: your bottom line and your reputation.

1. **Cybersecurity gaps** - Unapproved apps may lack strong security controls like MFA. Attackers love those weak spots.
2. **Compliance trouble** - If you are in accounting, law, or healthcare, one slip with client data in a non-compliant app can mean fines or lost trust. The Illinois Attorney General explains what happens after a breach and what businesses must do on its Data Breach Reporting for Businesses page.
3. **Data loss** - If someone stores sensitive files in a personal app and then leaves the company, you might never see that data again.
4. **Hidden costs** - Fixing the mess after a Shadow IT incident, recovering lost data, paying ransomware, and handling PR damage can cost far more than investing in proper IT management upfront.

cont...

The Hidden Dangers of Shadow IT

How to Spot Shadow IT

Shadow IT often hides in plain sight. You might notice:

- Employees sending work files to personal emails
- “Free” software on company computers that IT did not install
- Cloud accounts created without IT approval

If you are hearing “Don’t worry, I am just using my own...” it is time to worry.

How to Protect Your Business

You cannot eliminate Shadow IT completely, but you can control it.

1. Create an approved app list.
2. Give your team safe, approved tools. If they know what is available, they are less likely to go rogue.
3. Make security easy.
4. Streamline logins with single sign-on and MFA so the secure path is also the simple path.
5. Educate your team.
6. Share local stories and clear rules. People make better choices when they understand the risk.
7. Monitor your network.
8. An MSP can spot unmanaged apps and devices before they cause harm.
9. Have a clear policy.
10. Keep it short, plain, and easy to follow. For practical guidance on reducing Shadow IT, the UK’s National Cyber Security Centre has a helpful, free guide: Shadow IT: identify and reduce it.

Bottom Line

Shadow IT is not just a tech problem. It is a business risk. The good news is that with the right safeguards, you can protect your company without becoming the “IT police.”

Is Your Business on the Dark Web?

Would you know if your company's login credentials were already for sale on the dark web?

Most breaches don't start with a dramatic hacker breaking down digital walls. They start with something much quieter, a leaked email and password combo, floating around in a shady corner of the internet where cybercriminals shop like it's Black Friday.

That's where dark web monitoring comes in. And if you don't have it, you're flying blind.

What Is the Dark Web—and Why Should You Care?

The dark web is like the black market of the internet. It's hidden from standard browsers and search engines, and it's where cybercriminals buy and sell everything from Social Security numbers to banking logins to business email credentials.

Here's the scary part: Small businesses are prime targets.

Why? Because you've got data worth stealing, but often not the resources to detect the threat early. That's where dark web monitoring steps in. It acts like a watchtower, constantly scanning criminal marketplaces, private forums, and data dumps looking for your company's information.

What Dark Web Monitoring Does (And Why It Matters)

With dark web monitoring in place, here's what you get:

- Real-Time Alerts: If one of your employee's emails and passwords pop up on the dark web, you're notified, immediately.
- Proactive Protection: You can force a password change before a breach happens, not after.
- Risk Reduction: Many breaches start with a single compromised account. Spotting it early prevents a domino effect.
- Peace of Mind: It's one less thing to worry about when you're already juggling a million fires.

Most business owners don't have the time or tools to monitor these shady corners of the internet. And by the time you do find out about a breach? It's usually because a client emails you saying something weird is going on.

It's Not Just Big Companies Being Targeted

I hear this a lot: "We're small. Why would anyone target us?"

Cybercriminals don't care about your size. They care about how easy you are to exploit. And with remote work, reused passwords, and business emails being the golden key to everything from accounting software to payroll, your team is vulnerable.

Especially if you don't know what's already been leaked.

DMARC: Why It Matters Now More Than Ever

If your business relies on email to communicate with clients, vendors, or partners, your ability to reach their inbox is under threat. In 2025, major providers like Microsoft and Google are strictly enforcing a protocol called DMARC, and if it's missing or misconfigured, your messages may never make it through.

Whether you're sending invoices, follow-ups, marketing emails, or support updates, failing to configure DMARC properly could mean your business emails are flagged as spam, blocked entirely, or worse, spoofed by cybercriminals.

Let's break down what DMARC is, why it matters, and what you need to do today to keep your communications flowing.

What Is DMARC?

DMARC stands for Domain-based Message Authentication, Reporting and Conformance. It works alongside two other email security tools—SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail)—to verify that the emails sent from your domain are legitimate.

In plain terms, DMARC tells receiving email systems, "This message really came from my domain," and provides instructions on what to do if that claim cannot be verified.

Why Email Deliverability Is at Risk

Email is one of the top ways businesses communicate. But in recent years, phishing attacks and email spoofing have become increasingly sophisticated. Cybercriminals can send messages that appear to come from your domain, tricking customers, vendors, or employees into clicking malicious links or sharing sensitive information.

According to AppViewX, DMARC helps stop these attacks before they reach inboxes. It ensures only verified emails get delivered and tells providers what to do with anything suspicious.

Starting in 2025, email giants like Gmail, Yahoo, and Microsoft are blocking or quarantining messages that don't comply with DMARC. If your DMARC record is missing or incorrect, your emails could get flagged, even if you're sending legitimate messages.

The Business Impact of Not Having DMARC

- Emails may never reach your clients. Important communication can go to spam or get blocked entirely.
- Your domain can be impersonated. Hackers can spoof your email address to scam clients or suppliers.
- You could face compliance issues. Standards like PCI DSS v4.0 now require DMARC for organizations handling cardholder data.
- Your brand reputation suffers. If your domain is used in phishing attacks, people will lose trust in your organization.

Real-world cases show organizations that implement DMARC see improved deliverability, reduced spoofing attempts, and better security outcomes across the board.

DMARC: Why It Matters Now More Than Ever

DMARC in Action: How It Works

DMARC allows your domain to do three important things:

1. Authenticate who can send messages using your domain.
2. Instruct receiving email servers to either deliver, quarantine, or reject unverified messages.
3. Report on who is trying to send messages on your behalf, giving you visibility into misuse or misconfigurations.

This combination makes DMARC a powerful tool for protecting your domain and email reputation.

Why This Is Urgent in 2025

Microsoft began strict DMARC enforcement in May 2025, with Gmail and Yahoo following suit. If you send bulk emails or rely heavily on email marketing, the consequences of non-compliance are immediate. Even transactional emails like invoices or meeting invites could bounce if your DMARC isn't correctly set up.

Organizations that send more than 5,000 emails per day must implement DMARC or risk getting blacklisted. That means even mid-sized businesses are affected, not just large corporations.

DMARC Setup: What You Need to Do

1. Start with SPF and DKIM. These two records validate your email sources and are required for DMARC to work.
2. Publish a DMARC policy. Begin with a monitoring policy (p=none) to gather data without blocking emails.
3. Review reports. Use DMARC aggregate (RUA) reports to see who is sending email on your behalf.
4. Move to enforcement. Once you're confident in your setup, transition to stricter policies like quarantine or reject.
5. Keep it updated. Email vendors, services, and platforms can change. Regular reviews ensure your records stay accurate.

For organizations managing multiple domains or vendors, using a DMARC management tool can simplify this process and provide real-time insight.

DMARC Is Not Optional Anymore

In 2025, DMARC has become the standard for protecting email communication, preventing fraud, and ensuring your messages actually reach the people who need them.

Without it, you are risking email outages, reputational damage, and lost trust.

REFER TO ESCAPE:

YOU COULD WIN A $2,500 VACATION!

For a limited time, every qualified referral you send enters you to win a $2,500 travel voucher through House of Travel, redeemable for a vacation of your choice

Hurry—Entries Close September 16th, 2025!

More details and official rules on our website.

GOLEADINGIT.COM/REFER-TO-ESCAPE

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

LeadingIT Core Values Victor of the Month

Congratulations to Geovel, this month's Values Victor at LeadingIT for being Driven!

Geovel consistently brings a strong work ethic, a solution-focused mindset, and a commitment to growth. He demonstrates what it means to be driven: showing up, working hard, and doing what it takes to support our clients and our team.

Our company grows because our people do, and Geovel is a great example of that in action. Well done, Geovel!

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

GEOVEL OPERANA	9/9
MATTHEW PEPPIN	9/11
KELLY KONTAXIS	9/12
MATTHEW MCMULLAN	9/24