ANDRE BROWN · DATA SECURITY STRATEGIST

IT Assessment Findings

Northline Supplies — example walkthrough

How I turn a messy tech setup into plain-language priorities and a plan your team can actually finish in 30 days.

andrenbrown.com
Composite example drawn from common small-business patterns — not a named client file.

A quick note before the findings

When someone asks what an assessment from me looks like, I don’t hand them a blank template. I show them the kind of write-up leadership can read in one sitting: what’s going on, what’s already fine, what I’d fix first, and what can wait.

Northline Supplies is a stand-in — an 18-person wholesale shop with Microsoft 365, QuickBooks, a file server, and the usual “one person who knows how everything works.” The issues below are the ones I see most often. Your report would use your systems, your people, and your priorities.

> *“Most businesses don’t need a scare story. They need a short list, in order, and someone willing to help with the first few fixes.”*

— Andre Brown

Data Security Strategist

1. What I’d tell leadership

Northline can run day to day. Orders still move. Email still works. The risk isn’t that the lights are off — it’s that a stolen password, a failed disk, or one person out sick could slow the business more than anyone expects.

I’d start with three things: turn on a second login step for email, prove a backup can actually be restored, and stop sharing one admin password among several people. None of that requires a six-month project. It does require someone to own the next 30 days.

Who this example is about

Business	Wholesale distributor · ~18 people
Tools in play	Microsoft 365, QuickBooks Online, on-site file server, Windows PCs
What brought them in	Slow shared folders, insurance form due, IT knowledge in one head
How we’d work	Short conversations, a look at how things are set up, a written plan

2. What we look at — and what we don’t

I keep the first pass practical. The goal is a clear picture and a fix list — not a lab exercise.

In this review

- How people sign in to email and the main apps
- Who has full admin control, and whether passwords are shared
- Whether backups exist — and whether anyone has tested a restore
- How files are shared outside the company
- Whether devices get updates
- What happens if the usual IT contact is unavailable

Not in this first pass

- A formal penetration test
- A legal compliance stamp
- Rebuilding the warehouse network from scratch
- Standing up 24/7 monitoring

3. What’s already working

I always start here. It builds trust, and it stops us from “fixing” things that are fine.

What’s working	Why I leave it alone (for now)
Microsoft 365 is the hub for mail and documents	Better than work scattered across personal accounts
Accounting lives in QuickBooks Online	Not trapped on a single laptop
Customer work mostly stays on company email	Clearer ownership and fewer surprises
Leadership cares about the insurance / security story	You’ll actually finish a short plan

4. Findings — in the order I'd tackle them

Critical = days · **High** = this month · **Medium** = this quarter

Critical

ID	Finding	Why it matters	First step
C1	**Most people don't have MFA on Microsoft 365**	One stolen password can open email and unlock other systems	Turn MFA on this week — owners and anyone near banking first
C2	**Backups exist, but nobody's tested a restore in over a year**	You may find out too late that recovery doesn't work	Restore one real folder and one cloud file; write down what happened

High

ID	Finding	Why it matters	First step
H1	**One shared admin password** for the file server	Any leak becomes everyone's problem; hard to see who changed what	Named admin logins + a password manager; retire the shared note
H2	**An old contractor account** still active in Microsoft 365	Access you forgot about is still access	Turn it off; review guests and vendors the same week
H3	**"Anyone with the link"** used for customer price sheets	Links travel farther than you intend	Share to specific people; clean up old public links

Medium

ID	Finding	Why it matters	First step
M1	**Almost all IT know-how sits with one person**	Vacation or turnover becomes a business problem	One-page handoff: who to call, where things live, how to restart shares
M2	**A few PCs are months behind on updates**	Known bugs stay open longer than they should	Turn on automatic updates; patch the oldest machines first
M3	**Shared folders have years of clutter**	People waste time and grab the wrong version	Agree a simple layout for new files; archive the old pile gradually

5. The 30-day plan I’d recommend

Three commitments. If we try to do everything, we’ll finish nothing.

#	What we’ll finish	By when	Who owns it
1	MFA on for every Microsoft 365 user (owners and finance first)	Day 7	Office manager, with guidance
2	One proven file restore and one cloud-file restore, written down	Day 14	IT contact + a backup owner
3	Named admins, password manager, old contractor removed, public links reviewed	Day 30	IT contact + owner

How the month can look

- **Week 1** — MFA live; list of admins and guest accounts in one place
- **Week 2** — Restore tests done; results on a single page
- **Week 3** — Shared server password gone; password manager in use
- **Week 4** — Public links cleaned up; short handoff notes written; insurance answers updated

We’ll park for later

- Replacing the file server
- A new monitoring product
- Warehouse Wi-Fi redesign
- Custom software

6. If an insurer or customer asks

After this month, Northline could answer common questions without hand-waving:

- **MFA on email?** Yes — rolled out for staff accounts.
- **Do you test backups?** Yes — restore test on file, with a date.
- **What happens when someone leaves?** Named steps to remove access the same day.