continued from page 3....

- Faster paperwork: tools like Microsoft 365 Copilot can draft quotes, summarize shift notes, write up work orders and pull answers from long manuals or specs.
- Smarter planning: AI can help forecast demand and inventory using the sales and production data you already have.

The catch: AI works best on a solid foundation.

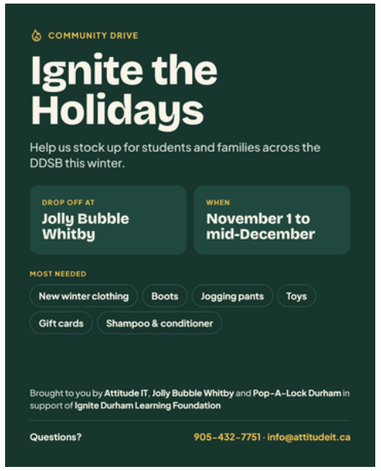
A 2026 Statistics Canada study found that businesses using AI were about 17% more productive than those that weren't. But much of that advantage came from the groundwork those businesses had already done, like using cloud systems, data analytics and staff technology training.

Once researchers accounted for that groundwork, the direct boost from AI alone was much smaller. In other words, AI doesn't fix messy processes. It speeds up good ones. The businesses getting the most *from* AI are the ones that cleaned up their data and digitized their paperwork first.

Small changes that add up

- Digital forms for timesheets, inspections and safety checks that feed straight into your systems
- Shared cloud folders so the office and the field always see the same version
- Simple automation, like approvals or notifications that happen without someone chasing them
- Reporting dashboards that show job costs or production numbers without building a report by hand
- Reliable connectivity where the work actually happens

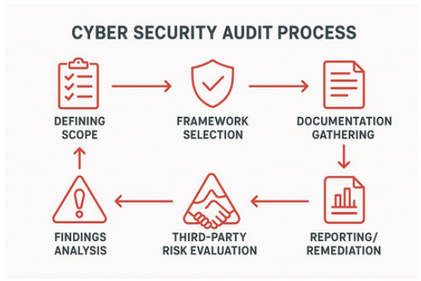
Each one also lays the groundwork for AI down the road.



Your 2027 challenge

Pick one repetitive task. For one week, have the team note every time they do it and how long it takes. You'll have a clear picture of what automating it is worth, and a great place to start.

Business risk: You Trust Your Vendors. But Do You Know How They Protect Your Data?



Your business might have strong security, but your data doesn't only live with you. It's in your payroll system, your accounting software, your CRM, your cloud storage and with any contractor who logs into your systems.

If one of those vendors has a breach, it can expose your information just as easily as a breach of your own.

Why vendors are a target

Attackers know that breaking into one supplier can open the door to hundreds of its customers.

A payroll provider, an IT tool or a shared file platform holds data from many businesses at once, which makes it far more valuable than any single company.

Why this matters here: under PIPEDA, your business remains responsible for personal information about customers and employees even when a vendor handles it on your behalf.

Five questions to ask any vendor that handles sensitive information

1. Do you use multifactor authentication and encrypt our data?
2. Where is our data stored, and is it kept in Canada?
3. Who on your team can access it, and how is that controlled?
4. If you have a breach, how and how quickly will you tell us?
5. What happens to our data if we stop working together?

A trustworthy vendor will be glad you asked. If the answers are vague, that tells you something too.

Optional: Attitude IT can help you review your key vendors and flag where your data may be at risk. Receive an easy to review report with recommendations for your vendors. Ask us about a Vendor Cybersecurity Risk Audit.

ATTITUDE CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably



Your 2027 IT Budget Doesn't Need to Be Bigger. It Needs to Be Smarter

Every fall, the same advice makes the rounds: spend less on technology next year. But for most small and mid-sized businesses, the problem isn't how much they spend. It's where the money goes. Or the resources are missing to be able to take advantage of funding, new processes etc.

The data tells a clear story. Businesses are quietly overpaying for tools they don't use, while underspending on the protections that would save them the most.

Where the money leaks

Software nobody uses. In Flexera's 2025 State of IT Asset Management report, IT professionals estimated that 25% to 30% of their IT budgets are wasted on redundant tools and underused licenses. Zylo's 2026 SaaS Management Index found that only about 54% of purchased software licenses were actively used in 2025.

licenses still assigned to people who left, overlapping apps that do the same job, and subscriptions nobody remembers signing up for.

Rising subscription costs.

Microsoft raised prices on most commercial Microsoft 365 plans on July 1, 2026, and most businesses feel it at their next renewal. Paying for the wrong plan, or the wrong number of users, now costs more than it did a year ago.

proper onboarding and offboarding procedures can help mitigate these costs. Planning what role needs what level of license and for areas with high turn over planning for monthly licenses instead of annual can help reduce costs.

we spoke with a business recently as they considered downgrading their plan. They had no idea there were so many features that they were not taking advantage of from one of their platforms and it allowed them to remove a different subscription that was more costly.

Paying for recovery instead of prevention.

Statistics Canada found that total spending on recovery doubled, from about $600 million in 2021 to $1.2 billion.

Meanwhile, just over 1 in 4 Canadian businesses have written cybersecurity policies in place. The cost of cleaning up is rising much faster than the cost of preventing.

Emergency replacements

A computer that fails without warning costs more than one replaced on schedule: rush pricing, lost work and an afternoon of downtime. And with demand for AI data centers pushing up the price of memory chips and processors, waiting until hardware breaks is getting more expensive.

Time lost to manual work. Double data entry, paper forms and spreadsheets emailed back and forth never show up on an invoice, but they cost hours every week.

Older equipment is susceptible to security gaps as regular patching can not be completed. You can always repurpose equipment to an area that is not a security risk.

Time lost to manual work.

Double data entry, paper forms and spreadsheets emailed back and forth never show up on an invoice, but they cost hours every week. Consider implementing some small AI upgrades for those in roles that have a lot of repetative tasks. This will improve productivity and elevate your team to work on more important tasks.

Continued on page 2....

continued from page 1

Where to move the money

The smartest 2027 budgets don't grow. They shift:

- From unused licenses to the security features you're missing, like Conditional Access and stronger MFA
- From emergency replacements to a planned refresh schedule
- From recovery to tested backups and staff training
- From manual work to simple automation

In many cases, cutting the waste covers most of the cost of the upgrades.

Funding that can help Ontario businesses

You may not have to cover the full cost of upgrades yourself. Both the Ontario and federal governments are putting new money behind technology and AI adoption, especially since Canada launched its national AI strategy, AI for All, in June 2026.

There is funding available for AI adoption, next gen manufacturing and supply chain innovation. these grants are available through BDC and the government of Ontario. Check out FedDev Ontario for a list of available grants and innovation clusters.

AI & productivity: Your Business Is Already Using AI. Do You Know Where?

Ask your team whether they use AI at work and you might be surprised. Someone is drafting emails in ChatGPT. Someone else is summarizing meeting notes in Copilot, or using a free tool to clean up a spreadsheet.

That's not a bad thing. AI can save real time on everyday tasks. The challenge is that most of it is happening without clear guidelines, and that's where the risk comes in.

2027 IT BUDGET HEALTH CHECK

Give yourself one point for every statement that's true for your business today.

- ☐ 1. Every user, including the owner, has MFA turned on
- ☐ 2. We have tested restoring from a backup in the last 3 months
- ☐ 3. Our backups include a copy kept off-site or offline
- ☐ 4. We reviewed our Microsoft 365 licenses in the last 6 months
- ☐ 5. No licenses are still assigned to former employees
- ☐ 6. Only a few people have administrator access
- ☐ 7. We replace computers on a planned schedule, not when they fail
- ☐ 8. Our team had security awareness training this year
- ☐ 9. We know who to call, and what to do, if our systems go down
- ☐ 10. We have clear rules for which AI tools staff can use

MY SCORE: _____ / 10

9 to 10	7 to 8	0 to 6
Strong foundation	On track, a few gaps	Time for a plan

Scored under 7? Let's talk.

Book a complimentary 20-minute Technology Planning Conversation with Attitude IT.

905-432-7751 · info@attitudeit.ca · www.attitudeit.ca

Where the risk is

- Data privacy: free consumer AI tools may store what's typed in. Client names, pricing or financials pasted into the wrong tool can leave your control.
- Accuracy: AI can sound confident and still be wrong. A quick human check before anything goes to a customer matters.
- Inconsistency: when everyone uses a different tool, nobody knows what's being shared or where.

Adopting AI with confidence

You don't need a 20-page policy. Start with a short, clear one. IE What is your company approved AI Tool.

Business tools like Microsoft 365 Copilot keep your data inside your account. which makes them a safer starting point than free alternatives.

Ontario note: since January 1, 2026, employers with 25 or more employees must say in publicly advertised job postings if they use AI to screen, assess or select applicants.

Three questions to ask your team

- Which AI tools are you using for work right now?
- What kind of information are you putting into them?
- Who checks the results before they're used?

The answers will tell you exactly where to start.

Cybersecurity spotlight: Your Password Wasn't Stolen. So How Did Someone Get Into Your Email?

When an email account gets hacked, the first question is usually "Whose password was stolen?" Increasingly, the answer is nobody's. Attackers have found ways in that skip the password altogether.

How they get in

- Stolen sign-in sessions: a fake login page passes your real password and MFA code to Microsoft, then keeps the "you're signed in" session for itself. The attacker is in without ever needing your password again.
- MFA fatigue: the attacker triggers sign-in prompt after prompt until someone taps "Approve" just to make it stop.
- Risky third-party apps: a convincing request asks you to "allow access" for a calendar, PDF or file-sharing app. Once approved, that app can read your mailbox without a password.
- Old sign-in methods: older connections that don't support MFA can still be used if they haven't been turned off.



What actually stops it

- Conditional Access: rules for who can sign in, from where and on what device. A stolen session from another country or an unknown laptop gets blocked.
- Stronger MFA: number matching or passkeys instead of a simple "Approve" tap.
- Locked-down admin accounts: separate admin accounts with the strictest rules, so one phished user can't take over everything.
- App consent controls: only IT can approve apps that want access to company data.

Quick Microsoft 365 security checklist

- MFA is on for every user, including the owner
- Sign-ins from outside Canada are blocked or reviewed
- Older sign-in methods are turned off
- Admin access is limited and on separate accounts
- Staff can't approve third-party apps on their own



Manufacturing & construction: The Hidden Cost of "We've Always Done It This Way"

Nobody puts "wasted time" on an invoice.

But in many shops, plants and job sites, it's one of the biggest costs in the business, and it's hiding in everyday routines.

Where the time goes

- Double data entry: paper timesheets typed into payroll, job notes retyped into estimates, orders entered into two systems that don't talk to each other.
- Spreadsheets on the move: the "latest version" emailed back and forth until nobody's sure which one is right.
- Photos and documents on personal phones: job site photos, drawings and change orders scattered across devices instead of in one place.
- Slow or patchy networks: shop-floor or site-trailer Wi-Fi that drops out, so people wait, walk back to the office or give up and use paper.

Each one costs a few minutes. Multiply that by every person, every day, and it adds up to weeks of work a year.

How AI is helping manufacturers do more

AI adoption in Canada is climbing fast. Statistics Canada found that 19.2% of Canadian businesses used AI to produce goods or deliver services in the 12 months leading up to spring 2026, triple the 6.1% reported two years earlier. Hands-on industries are further behind: only 9.2% of construction businesses reported using AI, and manufacturers named a lack of skilled workers as a key barrier.

That gap is an opportunity. Here's where AI is already making a difference on the floor:

- Predictive maintenance: sensors and AI spot signs of wear before a machine breaks down. Industry research, including McKinsey's, has found this approach can cut machine downtime by 30% to 50%.
- Quality inspection: cameras paired with AI catch defects at line speed, reducing scrap and rework.

continued on page 4...