Virtual Dynamics

MANAGED IT SERVICES

A FREE GUIDE FOR BUSINESS OWNERS & OFFICE MANAGERS

The No-Nonsense IT Survival Guide

for Small Business

Security, right-sizing, real cost savings, and what to do when the cloud has a bad day.

INSIDE

Cyber threats · Breach costs & reputation · Right-sizing · Cost leaks · Cloud reality check · Backups · Business continuity · Self-assessment

PUBLISHED BY

Virtual Dynamics · Managed IT for Chicagoland since 2010

EDITION

2026

WELCOME

Hi. Let's make IT boring again.

Most small businesses don't have an IT department. They have **a person**, often the office manager, the owner, or "the one who's good with computers," plus a pile of logins, a closet with blinking lights, and a vague feeling that something important isn't backed up.

This guide is for that person. It's written in plain English, it uses real numbers from credible sources, and it'll show you where the biggest risks hide, where money quietly leaks out, and what to fix first.

You don't need to do everything at once. Read the page that worries you most, try the **self-assessment on page 12**, and pick three things to fix this quarter.

> **How to use this guide:** Each section ends with a short "Do this week" list. If you only read those, you'll still be ahead of most businesses.

88% of breaches at small and mid-sized businesses involved ransomware, compared with 39% at large organizations.

Verizon 2025 DBIR

What's inside

Cyber threats, part 1: ransomware 03

Cyber threats, part 2: the con artists 04

Security basics that actually work 05

What a breach really costs (money and reputation) 06

Right-sizing: stop paying for shelfware 07

Where IT money leaks 08

Cloud is great... until it isn't 09

Backups & disaster recovery 10

Business continuity: when the office goes dark 11

Self-assessment & questions to ask any MSP 12

Glossary & sources 13

About Virtual Dynamics 14

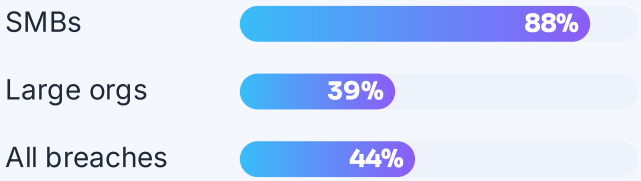
CYBER THREATS · PART 1

Ransomware: the small-business tax nobody voted for

Spoiler: paying doesn't guarantee you get your data back, and it marks you as someone who pays.

Ransomware locks up (and increasingly steals) your data, then demands payment. The myth is that criminals only chase big companies. The data says the opposite: smaller businesses are hit *more*, because their defenses and backups are usually thinner.

Share of breaches involving ransomware



Verizon 2025 DBIR. SMB = fewer than 1,000 employees.

$115K
median ransom paid (down from $150K)
Verizon 2025 DBIR

64%
of victim organizations did not pay the ransom
Verizon 2025 DBIR

+37%
rise in ransomware presence in breaches vs. the prior year
Verizon 2025 DBIR

$5.08M
average cost of a ransomware/extortion incident disclosed by the attacker
IBM Cost of a Data Breach 2025

How it usually gets in

Stolen passwords
Credential abuse was the #1 initial way in (22% of breaches).

Unpatched systems
Exploited vulnerabilities: 20% of breaches, up 34%, often VPNs and firewalls.

One bad click
Phishing emails that drop malware or harvest logins.

Initial-vector figures: Verizon 2025 DBIR news release.

Do this week: turn on MFA for email and remote access · confirm your firewall/VPN firmware is current · ask "when did we last *test* a restore?" (If the answer is a shrug, see page 10.)

CYBER THREATS · PART 2

The con artists: phishing, fake invoices & cloned voices

Criminals stopped breaking in. Now they just ask nicely and wear a convincing costume.

Most attacks don't need genius hackers. They need a busy person, a believable message, and a little urgency. The Verizon DBIR found the **human element in about 60% of breaches**. That's not because people are dumb; it's because criminals are good at being convincing.

The greatest hits

- **Business email compromise (BEC):** "Hi, it's the CEO, wire this today," or a vendor's "new bank details." It cost U.S. victims **$2.77 billion** in 2024 (FBI IC3).
- **Credential theft:** fake Microsoft 365 login pages, reused passwords, password-stealing malware.
- **AI voice and deepfakes:** the FBI warned in May 2025 that criminals are using **AI-generated voice messages** to impersonate trusted people. Your "boss" on voicemail may not be your boss.
- **Vendor and supplier compromise:** third-party involvement in breaches **doubled from 15% to 30%** (DBIR). Your weakest link may be someone else's.
- **Honest mistakes:** the wrong attachment, the wrong recipient, a shared folder set to "anyone with the link."



Verizon 2025 DBIR



Verizon 2025 DBIR (up from 15%)

$2.77B

reported BEC losses in 2024; total cybercrime losses reported to IC3 were **$16.6B**, up 33%.

FBI IC3 2024 Internet Crime Report

The callback rule: any request to change bank details, buy gift cards, or rush a payment gets verified by calling a number you already have, never the one in the message. It's free, takes 2 minutes, and beats most BEC and deepfake scams.

SECURITY

Security basics that actually work (and what your insurer will ask)

Six controls. One afternoon of honesty. Fewer sleepless nights.

You don't need a fortress. You need the handful of controls that stop the most common attacks, and the paperwork to prove you have them. Conveniently, those are the same things cyber-insurance carriers now ask about before they'll quote or renew a policy.

The cyber-insurance short list

- [ ] **MFA everywhere**
  email, remote access, admin & cloud accounts
- [ ] **EDR on every device**
  modern endpoint detection, actually monitored
- [ ] **Tested backups**
  immutable/offline copies with dated restore tests
- [ ] **Patching on a schedule**
  especially firewalls, VPNs and servers
- [ ] **Security training**
  phishing awareness with completion records
- [ ] **Written incident response plan**
  who calls whom, reviewed yearly

Commonly requested controls; requirements vary by carrier and policy. Sources: QOS MSP and Scopable cyber-insurance requirement summaries (see page 13). Your broker and policy are the final word.

Why MFA first?

Stolen credentials are the top way attackers get in. A second factor turns a stolen password into a useless one most of the time.

Patching isn't optional

Exploited vulnerabilities rose **34%**, with a focus on edge devices like VPNs. That box in the closet counts.

Verizon 2025 DBIR

Train like it's a fire drill

Short, regular phishing training beats one annual video everyone watches on mute.

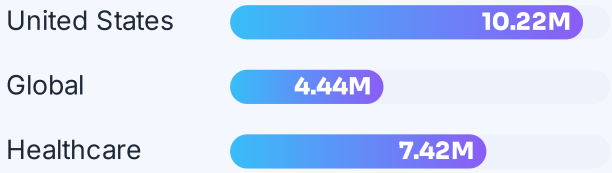
Do this week: pull last year's cyber-insurance application and check every "yes" is actually true today. A "yes" that isn't true can become a denied claim. **Not legal advice**

COSTS & REPUTATION

What a breach really costs: money, customers and reputation

The ransom is the cheap part. Lost customers are the expensive part.

Average cost of a data breach (USD millions)



IBM Cost of a Data Breach 2025. Healthcare figure is the global industry average.

Where the money goes (global avg, $M)



IBM Cost of a Data Breach 2025. "Lost business" includes downtime, lost customers and reputation damage.

Those are averages across organizations larger than most of our readers, but the *shape* applies to everyone: the biggest costs are figuring out what happened and the customers you lose, not the ransom.

Reputation: the cost that doesn't show up on the invoice

70%

of U.S. consumers say they'd stop shopping with a brand after a security incident

Vercara Consumer Trust & Risk Report, Dec 2024

58%

believe a breached brand is not trustworthy

Vercara, Dec 2024

38%

of U.S. fraud victims cut all ties with the brand; 33% warn friends and family

Telesign Trust Index, Nov 2024

Disclosure isn't optional

Illinois' Personal Information Protection Act requires notifying affected residents of many breaches, and HIPAA's Breach Notification Rule applies to health data. Other states and industries have their own rules. A breach can become public whether you like it or not. **Not legal advice**

Reviews remember. One "they lost my data" review sits next to your 5 stars for years. The cheapest reputation management is not getting breached, and having a plan if you do.

RIGHT-SIZING

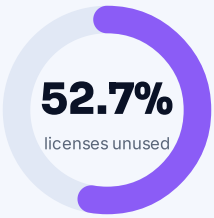
Right-sizing: stop paying for shelfware

If nobody has logged in since the holiday party, it's not a license. It's a donation.

"Right-sizing" means paying for what you actually use, no more and no less. Most businesses drift into overspending one reasonable decision at a time: the premium license "just in case," the departed employee whose mailbox is still billing, the server bought for a growth plan that changed.

Where to look

- **Licenses:** match Microsoft 365 / Google Workspace plans to roles. Not everyone needs the top tier.
- **Ex-employees:** disable accounts on day one (it's a security issue too), then reclaim or convert the license.
- **Duplicate apps:** three file-sharing tools and two video platforms? Pick one.
- **Hardware:** replace on a schedule, not in a panic. Overbuying servers "for later" ties up cash in metal.
- **Aging Windows PCs:** Microsoft ended Windows 10 support on **Oct 14, 2025**. Unsupported machines stop getting security fixes. Plan upgrades or replacements instead of waiting for a crisis.



52.7% of purchased SaaS licenses went unused over a 30-day window.

Zylo 2025 SaaS Management Index (enterprise data)

$21M

average annual spend on unused SaaS licenses per organization in Zylo's dataset. Your number is smaller; the percentage often isn't.

Zylo 2025

Do this week: export your Microsoft 365 or Google Workspace user list. Highlight anyone who left, anyone sharing a login, and anyone on a plan bigger than their job. That spreadsheet is usually worth real money.

COST REDUCTION

Where IT money leaks (and how to plug it)

Predictable costs aren't just nicer. They're usually smaller.

Break-fix surprises

Hourly bills arrive after the outage, when you have no leverage.

Downtime

Staff who can't work still get paid. Customers who can't reach you call someone else.

Repeat problems

Fixing the same issue monthly instead of fixing the cause.

Vendor sprawl

Five vendors, five invoices, five people blaming each other.

Shelfware

Unused licenses and duplicate apps (page 7).

Emergency buying

Rush-shipped replacement hardware at full price.

Break-fix vs. managed IT: the incentive problem

Break-fix	Managed (flat monthly)
✕ Provider earns more when things break	✓ Provider earns the same, so prevention pays
✕ Unpredictable monthly cost	✓ Budgetable, per-device or per-user pricing
✕ No one watching between calls	✓ 24/7 monitoring and patching
✕ Fixes symptoms	✓ Fixes root causes and plans upgrades

Budget rule of thumb

Ask for a price you can multiply: *per device × devices + per server × servers*. If a quote needs a decoder ring, keep asking questions.

Read the fine print for

Long auto-renewing terms, cancellation fees, "projects" that are really maintenance, and after-hours rates.

Do this week: add up the last 12 months of IT invoices, emergency purchases and software subscriptions. Most owners are surprised by the total. That's your baseline for any comparison.

CLOUD REALITY CHECK

Cloud is great… until it isn't

The cloud is just someone else's computer, with someone else's outage schedule.

The cloud is genuinely great: no server closet, work from anywhere, someone else patches the data center. But "in the cloud" doesn't mean "handled." Here's what the brochures skip.

☁ Outages happen to everyone

In July 2024 a faulty CrowdStrike update crashed an estimated **8.5 million Windows devices** worldwide, grounding flights and stalling businesses. Cloud and SaaS providers have bad days too. Have a plan B for email, phones and key apps.

Microsoft Official Blog, Jul 20 2024

💸 Runaway bills

Organizations estimate **27%** of their cloud infrastructure spend is wasted, and they exceed cloud budgets by **17%** on average. Idle servers and oversized instances bill 24/7.

Flexera 2025 State of the Cloud Report

🔒 Lock-in

Proprietary formats, egress fees and long commitments make leaving expensive. Before you move in, know how you'd move out: export formats, data ownership, exit costs.

🗂️ Your data, your responsibility

Microsoft's own Services Agreement recommends that customers regularly back up their content. Deleted-item retention isn't a backup. Back up Microsoft 365 and Google Workspace with a separate tool.

Microsoft Services Agreement

When on-prem or hybrid still makes sense

- Large files on a slow or expensive internet connection
- Line-of-business software that's built for a local server
- Predictable workloads where owning beats renting
- Compliance or latency needs that favor keeping data close



Flexera 2025

Do this week: confirm you have a third-party backup of email and files in Microsoft 365 / Google Workspace, and that someone can name the restore steps.

BACKUPS & DISASTER RECOVERY

Backups that actually restore

Schrödinger's backup: it both works and doesn't, until you try to restore it.

Everyone "has backups." Far fewer have backups they've **restored from recently**. A backup you've never tested is a hope, not a plan. Insurers increasingly want dated restore-test records, not just "yes, we back up."

The 3-2-1 rule (plus one)

3	2	1	+1
copies of your data	different types of storage	copy offsite / cloud	immutable or offline copy

That last "+1" matters because modern ransomware hunts for backups first. An immutable copy can't be changed or deleted, even by an admin account that's been compromised.

Back up more than files

- Microsoft 365 / Google Workspace mail, OneDrive, SharePoint, Drive
- Line-of-business databases (accounting, practice management, ERP)
- Server images, so you can restore the whole machine
- Firewall & network configs
- The passwords to the backup system itself (stored safely!)

Test like you mean it

Quarterly: restore a random file, a mailbox and one full system. Write down the date and how long it took. That time is your real recovery time.

Do this week: pick one important file from last month and ask for it back. Time it. If it takes more than an afternoon, or nobody knows how, you found your next project.

BUSINESS CONTINUITY

When the office goes dark: business continuity in plain English

Hope is not a strategy. A one-page plan is.

Business continuity is simply deciding, *before* the bad day, how you'll keep serving customers during one. Start with four scenarios:

The office is unusable

Fire, flood, burst pipe, construction. Can people work from home on day one?

The internet is down

Do you have a backup connection (a second ISP or a cellular failover)?

The power is out

UPS battery for network gear; laptops over desktops for key staff.

A key person is out

Who else knows the passwords, vendors and processes? Write it down.

RTO and RPO, minus the jargon

RTO

Recovery Time Objective: how long can you be down before it really hurts? "We can live without email for 2 hours, but not 2 days."

RPO

Recovery Point Objective: how much work can you afford to redo? Nightly backups = up to a day of lost work. Is that okay for your accounting system?

A one-page incident response plan

1. **Who decides:** the person who declares "this is an incident."
2. **Who to call:** IT provider, cyber insurer (often *before* anything else), attorney, bank.
3. **Contain:** disconnect affected machines; don't wipe evidence.
4. **Communicate:** what staff, customers and vendors hear, and from whom.
5. **Recover:** restore in priority order (your RTO list).
6. **Learn:** a short review afterward, then update the plan.

> **Do this week:** print the plan, plus key phone numbers, and keep a copy *off* the network. A plan stored only on the encrypted server is a very bad joke.

SELF-ASSESSMENT

The 5-minute IT self-assessment

Grab a pen. No one's grading you but you.

Check every box that's honestly true today

- [ ] MFA is on for email, remote access and every admin account
- [ ] Every computer has modern endpoint protection that someone monitors
- [ ] Updates install on a schedule (including firewall and VPN)
- [ ] We have an offsite and an immutable/offline backup
- [ ] We tested a restore in the last 90 days, and wrote down the date
- [ ] Microsoft 365 / Google Workspace data is backed up separately
- [ ] Departed employees lose access the same day
- [ ] Staff had phishing training in the last 12 months
- [ ] Payment/bank changes are verified by phone callback
- [ ] We have a written incident response plan (printed, off-network)
- [ ] We know our RTO and RPO for key systems
- [ ] Our IT costs are predictable month to month

Score it: 10-12 nicely done · 6-9 solid start, a few gaps · 0-5 you're in good company, and it's very fixable. Start with MFA and backups.

Questions to ask any IT provider (including us)

1. How fast does a real person respond?
Get a number, not 'quickly'.

2. What exactly is included in the monthly price?
Ask for exclusions in writing.

3. How long is the contract, and what does it cost to leave?
Watch for auto-renewal.

4. How do you test backups, and can I see a report?
Dated restore tests, not promises.

5. Who has admin access to our systems, and with MFA?
Your keys should not be a mystery.

6. Will you help with our cyber-insurance questionnaire?
Evidence, not checkboxes.

7. Who owns our passwords and documentation if we part ways?
You should.

REFERENCE

Glossary & sources

Plain-English glossary

BEC · Business email compromise: fraud using hijacked or spoofed email to redirect payments.

EDR / MDR · Endpoint detection & response; 'managed' when a team watches the alerts 24/7.

MFA · Multi-factor authentication: password plus a second proof like an app prompt.

Immutable backup · A backup copy that can't be altered or deleted for a set period.

RTO / RPO · How long you can be down / how much data you can afford to lose.

Patching · Installing security updates that fix known weaknesses.

Phishing / vishing · Fake emails / phone or voice messages designed to trick you.

Shelfware · Software you pay for but nobody uses.

vCIO · A part-time 'virtual CIO' who plans your IT roadmap and budget.

Hybrid cloud · Some systems in the cloud, some on-site, working together.

Sources

Verizon 2025 Data Breach Investigations Report (and SMB snapshot)
verizon.com/business/resources/reports/dbir

IBM Cost of a Data Breach Report 2025
ibm.com/reports/data-breach

FBI IC3 2024 Internet Crime Report
ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

FBI PSA I-051525-PSA, AI-generated voice impersonation
ic3.gov/PSA/2025/PSA250515

Vercara Consumer Trust & Risk Report (Dec 2024)
businesswire.com (Dec 12 2024 release)

Telesign Trust Index (Nov 2024)
businesswire.com (Nov 19 2024 release)

Zylo 2025 SaaS Management Index
zylo.com/news/2025-saas-management-index

Flexera 2025 State of the Cloud Report
flexera.com

Microsoft: CrowdStrike outage update (Jul 20 2024)
blogs.microsoft.com

Microsoft Services Agreement (backup recommendation)
microsoft.com/servicesagreement

Microsoft Windows 10 end of support
microsoft.com/windows/end-of-support

Cyber-insurance control summaries
qosmsp.com; scopable.io

Illinois Personal Information Protection Act (815 ILCS 530)
ilga.gov

HHS HIPAA Breach Notification Rule
hhs.gov/hipaa

Statistics reflect the cited reports as published; many draw on organizations larger than a typical small business and are included to show trends. This guide is general information, not legal, insurance or financial advice.

Virtual Dynamics
MANAGED IT SERVICES

ABOUT US

Want all of this handled by someone who picks up?

Virtual Dynamics has delivered managed IT for Chicagoland businesses since 2010: enterprise-grade IT at a small-business price. One partner for the whole stack, from the firewall to the cloud desktop, including virtual desktops at enterprise depth (Citrix, Azure Virtual Desktop, Windows 365, Omnissa Horizon).

53%

Average Savings. On average, our customers save about half of their total cost in IT and support services.

$50,000

Modernization in the cloud. Old servers replaced with a modern Microsoft Office 365 environment powering all six centers, saving $50,000 in the first year. *(Bobbie Noonan's Child Care)*

Upfront, no gimmicks pricing

User endpoints	**$39.00 / device / mo**
Servers	**$249.00 / server / mo**
Azure · Microsoft 365 · Google Workspace	**$399.00 / mo flat***
Routers, switches & firewalls	**$29.00 / device / mo**
Printers	**FREE (yes, even the jammy one)**

*Per platform managed, regardless of user count.

The No Shenanigans Promise

- Your first month is totally free
- No annual contracts
- No long-term commitments
- Savings that make you smile

What we take off your plate

- 24/7 monitoring & patching
- Help desk that picks up
- Security: MFA, EDR, training
- Encrypted backups powered by Acronis
- Microsoft 365 & Google Workspace
- Network, firewall & Wi-Fi
- Virtual desktops & cloud
- vCIO planning & budgets

Book your free IT assessment.

We'll run through page 12 with you and show you what to fix first. Zero jargon, zero pressure.

(888) 531-1109
vdcmsp.com