



Business Cybersecurity Checklist

A plain-English review of the protections most small organizations are expected to have. Written for owners and managers, not for technicians.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

You do not need to know how any of this works to use this checklist. Each item asks a simple question: does your organization have this, and has anyone actually checked it lately?

Some items will be things you handle yourself. Others will be things your IT provider handles for you. Either is fine. What matters is that somebody owns each one, and that you know which ones nobody owns.

How to use this document

Check an item only if it is **in place and somebody has confirmed it** in the past year. If you are assuming it is handled, leave it blank. Assumptions are the whole reason this checklist exists.

Blank items are not failures. They are your to-do list, and they are exactly the right thing to hand to whoever supports your technology.

A blank copy is safe to share. A filled-in copy is a map of your weak spots, so keep that one somewhere sensible.

The words you will hear, and what they actually mean

Multifactor authentication (MFA)

Signing in with your password plus a second thing, usually a code from an app on your phone. Think of a bank card: the card alone is not enough, and the PIN alone is not enough. CISA's Cross-Sector Cybersecurity Performance Goals place this near the top of the list, and so does this checklist.

Principle of least privilege

Everyone gets the access their job needs and nothing more. A hotel gives housekeeping a key that opens guest rooms, not the safe and the payroll office. Most organizations hand out the master key by accident.

Phishing

A message impersonating someone you trust, built to extract a password or redirect a payment. The digital version of somebody in a safety vest walking through a door because nobody wants to be the one who asks.

Business email compromise (BEC)

Phishing aimed specifically at money. Someone poses as a supplier, an executive, or a payroll contact and changes where a payment goes. No malware involved, which is exactly why filters do not stop it.

Ransomware

Software that encrypts your files and demands payment for the key. Someone changing the locks on your building and selling you the new key. Good backups are what turn this from a catastrophe into a bad week.

Patching

Installing the security fixes software makers release. Same idea as a recall notice on a car: the fault is known, the fix exists, and it only helps you if you actually book it in.

Attack surface

Everything you own that an attacker could try. Every extra account, device, and open connection is another door in the building, and every door needs a lock and someone who checks it.



1 Logins and Passwords

- ☐ Everybody has their own login. Nobody shares one.
Shared logins mean you can never tell who did what, and they keep working after somebody leaves.
- ☐ Administrative rights are separated from everyday accounts.
The people who can install software and change settings sign in to a second account to do it. If the administrator account is the one open all day in email, one bad click hands over the master key rather than a single room.
- ☐ Someone can tell you, today, who has those powerful logins. There is a list, and it is current.
- ☐ The passwords that came in the box have been changed on all your equipment.
This means your internet router and firewall, network switches, Wi-Fi, cameras, door systems, and printers. Factory passwords are published online.
- ☐ Staff know what a good password looks like here, because you told them.
Long is better than complicated. A phrase you can remember beats a short jumble you have to write down.
- ☐ There is an approved place to keep passwords.
Without one, they end up in spreadsheets, in email, and on notes under keyboards.
- ☐ When somebody leaves, their login is switched off that same day.

2 Two-Step Sign-In

If you fix one section this year, make it this one. A stolen password on its own is enough to sign in. A stolen password where multifactor authentication is enforced is not, because the attacker also needs the phone in your pocket. That is the whole idea, and it is why federal guidance keeps putting this first.

- ☐ It is turned on for email, and for your Microsoft 365 or Google account.
- ☐ It is turned on for anything reachable from outside the building.
Remote access into the office, and the tools used to support your computers from a distance.
- ☐ It is turned on for every powerful login, with no exceptions made for convenience.
Exceptions granted years ago for convenience are how most of these accounts get taken over.
- ☐ It is turned on for banking, payroll, and accounting.
- ☐ You know which accounts do not have it, and why.
Shared mailboxes and old automated accounts are the usual gaps.
- ☐ Codes come from an app or a small physical key rather than a text message, at least for the important accounts.
Text messages can be redirected to somebody else's phone. An app cannot.
- ☐ Somebody can get back in if a phone is lost or replaced.
Otherwise a broken phone locks you out of your own email.

3 Keeping Everything Up to Date

- ☐ Updates get installed on a schedule, not whenever a user finally stops clicking 'remind me later'.
Attackers routinely use flaws the manufacturer has already fixed. That is the entire premise of CISA's Known Exploited Vulnerabilities catalog, which is a published list of the holes being used right now.
- ☐ It is not just Windows. Web browsers, PDF readers, and the programs your business runs on are updated too.
These are attacked just as often as the operating system.
- ☐ Your equipment gets updates as well: firewall, internet router, Wi-Fi, network switches, cameras, and door systems.
- ☐ Somebody looks at which computers failed to update, and does something about it.
An update system nobody reads reports from is a reporting system, not a protection.
- ☐ Nothing in the building is past end of support.
End of life means the maker stopped selling it. End of support means they stopped fixing it, and that is the one that matters. Windows 10 reached end of support on October 14, 2025, so those machines are unprotected unless enrolled in Extended Security Updates, Microsoft's paid bridge. The first and cheapest year of the business version of that program ends October 13, 2026, and the price doubles each year after that.
- ☐ When something serious is in the news, it gets dealt with right away rather than waiting for the next scheduled round.

4 Protection on the Computers Themselves

- ☐ Every computer and server has security software on it, and somebody can see all of them in one place.
- ☐ Somebody would notice if one computer quietly stopped reporting in.
A machine that dropped off the list six months ago is the one that will cause the problem.
- ☐ Warnings are read by a person, not just written to a log nobody opens.
- ☐ Laptops have full-disk encryption switched on.
The whole drive is scrambled unless someone signs in properly, so pulling the drive out and reading it elsewhere gets you nothing. This is what turns a laptop left in a car into a lost laptop rather than a disclosure you have to report. On Windows this is usually BitLocker.
- ☐ The protection built into each computer is switched on, and was not turned off during some past troubleshooting.
- ☐ You have decided what you allow on USB flash drives and external drives, and staff know the answer.

5 Email

- ☐ Incoming mail is filtered for junk, scams, dangerous links, and dangerous attachments.
- ☐ Your domain has SPF, DKIM, and DMARC records published.
Three settings that let receiving mail servers check that a message claiming to come from you actually did. A wax seal on a letter: anybody can write your name on the envelope, but not everybody can produce the seal. You do not need to understand them, only to confirm somebody has set all three up.



- ☐ Mail cannot be quietly forwarded out of the organization without somebody knowing.
Setting up a secret forward is one of the first things an intruder does in a mailbox.
- ☐ Messages from outside the organization are visibly marked as outside.
This one small change makes it much harder to impersonate a coworker.
- ☐ Somebody would spot hidden rules in a mailbox, especially rules that hide or delete replies.
- ☐ Any change to bank details, payment instructions, or where a paycheck goes is confirmed by phone, on a number you already had.
This is business email compromise, and one redirected payment can cost more than any other incident on this list. There is no malware to detect and the money is rarely recoverable after the first day.

6 Backups

- ☐ You back up everything you would need to reopen for business.
Servers, the computers that matter, your business records, and your Microsoft 365 email and files. Cloud services are not automatically backed up for you.
- ☐ At least one copy is immutable or air-gapped.
Immutable means it cannot be altered or deleted for a set period, even by an administrator. Air-gapped means it is not reachable from your network at all. Either one is the fire safe rather than the filing cabinet next to the filing cabinet. Backups sitting on the same network, reachable with the same passwords, get destroyed along with everything else.
- ☐ Somebody checks that backups actually ran, and fixes them when they do not.
- ☐ Somebody has actually restored files from a backup and confirmed they opened.
A backup nobody has ever restored from is a hope, not a protection.
- ☐ You know roughly how long it would take to get running again, and how much recent work you would lose.
- ☐ You keep backups long enough to cover the way your business actually works, including anything you are required to retain.

7 Who Can See What

- ☐ Access to folders, files, and programs is based on the job somebody does now.
- ☐ Somebody reviews that access at least once a year.
Long-serving staff usually still hold access from every job they have ever had here.
- ☐ You know where your sensitive information actually lives.
Not where it is supposed to live. Where it is: on desktops, in personal cloud accounts, in old spreadsheets, on a laptop at somebody's house.
- ☐ Sensitive information is protected in a way that matches how sensitive it really is.
- ☐ Old computers, drives, and phones are properly wiped or destroyed before they leave, and you keep a record of it.
Deleting the files and reinstalling Windows is not enough.
- ☐ You have decided whether staff can use personal phones and laptops for work, and staff know the answer.

8 Your People

- ☐ Training happens more than once, and new hires get it when they start rather than a year later.
- ☐ Fake phishing tests, if you use them, are used to teach rather than to catch people out.
You want staff who report quickly, not staff who are afraid to admit a mistake.
- ☐ Everybody knows exactly who to tell when something looks wrong, and knows they will not be in trouble for telling you.
How fast somebody speaks up is the biggest single factor in how bad an incident gets.
- ☐ Everybody knows that nobody supporting your technology will ever ask for their password or a sign-in code.
- ☐ Owners, managers, and anyone who handles money get extra attention.
They are targeted by name, because they can approve payments.

9 Your Network and Your Building

- ☐ You know what is connected to your network, including the things nobody thinks of as computers.
- ☐ Guest Wi-Fi is separate from the network your business runs on.
- ☐ Cameras, door systems, and thermostats sit on a segmented part of the network.
Network segmentation means dividing one network into separate zones that cannot freely reach each other, the way a ship is built with watertight compartments. This equipment rarely gets updated and often ships with weak settings, so a compromised camera should not be able to reach your accounting system.
- ☐ Getting in from outside is limited to what is genuinely needed, and is protected rather than simply open.
- ☐ Server, network, and phone equipment is in a locked space.
- ☐ Visitors are accompanied anywhere they could see systems or records.

10 If Something Goes Wrong

- ☐ There is a printed contact list for a technology emergency.
Printed matters. A contact list stored only in the system that is down is not a contact list.
- ☐ Somebody is clearly allowed to make disruptive decisions in a hurry, such as shutting systems down.
- ☐ You know whether you carry cyber insurance, and what that policy expects you to have already done.
- ☐ You have found out in advance who you would be required to notify.
Rules under HIPAA, CJIS, state law, or a contract are much easier to read on a quiet Tuesday than during an incident.
- ☐ Leadership looks at technology risk at least once a year, alongside the other risks the organization carries.
- ☐ The outside companies with access to your systems have been looked at.
- ☐ Somebody other than the person who set it all up could work out how your systems fit together.
Write it down before you need it.

11 If Most of This Is Blank, Start Here

Do not try to do all of it. These five deliver the biggest real-world improvement for the least cost and disruption, and they are the order we would tackle them in.

No.	Do this	Because
1	Turn on two-step sign-in for email and every powerful login	Stops most break-ins that start with a stolen password, which is most of them.
2	Get one backup copy out of reach, and restore something from it to prove it works	Decides whether a bad day costs you an afternoon or several weeks.
3	Replace or retire anything running software that is no longer being fixed	These machines collect security holes that will never be closed.
4	Stop people using powerful logins for everyday work	Limits how far one bad click can spread.
5	Switch off departing staff logins the same day	One of the most common ways in, and one of the easiest to close.

■ Review record

Organization	Completed by
Date completed	Number of blank items
Next review date	

About this checklist

This is general guidance to help you have a better conversation about your technology. It is not an audit, and completing it does not make an organization compliant with HIPAA, CJIS, PCI DSS, the FTC Safeguards Rule, or any other set of rules. If your organization is subject to any of those, check them against the current published requirements and involve the right legal or compliance help.

The items here are drawn from public guidance including the NIST Cybersecurity Framework, the CISA Cybersecurity Performance Goals, and the CIS Critical Security Controls. All three are linked from the Computer Ties IT Resource Center, and all three remain the source of truth as they are updated.



Need help putting this into practice?

Computer Ties helps businesses, municipalities, and public-safety organizations across Michigan turn technology requirements into environments that are supportable day to day. If any item on this document raised a question you cannot answer internally, that is a good place to start a conversation.

NEW PROJECTS AND PLANNING
(517) 788-6393

EXISTING CUSTOMER SUPPORT
(517) 905-3168

2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990



Version 1.1 • September 2026 • © 2026 Computer Ties, LLC • General planning guidance, not legal, regulatory, or compliance advice.