FLYGHT

MANAGED IT SERVICES | TOLEDO, OHIO

The Small Business Cybersecurity Playbook

Everything You Need to Stop Being an Easy Target

A practical, no-BS guide to the cybersecurity essentials every small business needs — written in plain English for people who'd rather run their business than worry about hackers.

flyght.support | (419) 670-7100 | support@flyght.support

Why This Playbook Exists

Here's the uncomfortable truth: most small businesses are easy targets. Not because they're dumb, not because they don't care, but because nobody ever sat them down and explained what they actually need to do to protect themselves — in language that makes sense.

The cybersecurity industry loves to make things complicated. Three-letter acronyms, fear-mongering sales pitches, and solutions that cost more than your entire IT budget. It's enough to make most business owners throw up their hands and hope for the best.

Hope is not a strategy.

This playbook cuts through the noise. We're covering the seven essential security areas that every small business needs to address — not because we want to scare you, but because we want you to be informed, prepared, and in control. Each chapter explains what the technology does in plain English, why it matters to your business, what "good" actually looks like, and gives you a quick self-check to see where you stand.

You don't need to become a cybersecurity expert. You just need to know enough to ask the right questions and hold your IT provider accountable. That's what this guide is for.

What's Inside:

Let's get started.

01 MULTI-FACTOR AUTHENTICATION (MFA)

What It Is

Multi-factor authentication adds a second step when logging into your accounts. Instead of just a password, you also need something else — usually a code from your phone or an authenticator app. Think of it as a deadbolt on top of your door lock.

Why It Matters

Passwords get stolen. Period. They get phished, guessed, reused from breached databases, or simply written on sticky notes. MFA means that even when (not if) a password is compromised, the attacker still can't get in without that second factor. Microsoft estimates MFA blocks 99.9% of automated account attacks.

What "Good" Looks Like

- MFA is enabled on every business-critical application — email, cloud storage, accounting software, remote access, and admin portals.
- You're using an authenticator app (like Microsoft Authenticator or Duo) rather than SMS codes, which can be intercepted.
- Your IT provider has enforced MFA at the policy level, so individual users can't opt out or skip it.
- New employees are set up with MFA on day one as part of onboarding.

Quick Self-Check

- [ ] MFA is enabled on all email accounts
- [ ] MFA is enabled on cloud storage and file sharing (OneDrive, SharePoint, Google Drive)
- [ ] MFA is enabled on remote access tools (VPN, RDP, remote desktop)
- [ ] MFA is enforced on admin and privileged accounts
- [ ] We use an authenticator app, not just SMS codes
- [ ] MFA enrollment is part of our employee onboarding process

> *If your IT provider hasn't already enforced MFA across your organization, that's a red flag. This is table-stakes security in 2025 — it should have been done yesterday.*

02 ENDPOINT DETECTION & RESPONSE (EDR)

What It Is

EDR is the next generation of antivirus. Traditional antivirus works like a bouncer with a list of known troublemakers — it only blocks threats it recognizes. EDR works differently. It watches how programs behave in real time and flags anything suspicious, even threats that have never been seen before. It also gives your IT team the ability to investigate and respond to incidents remotely.

Why It Matters

Modern cyber threats are designed to slip past traditional antivirus. Ransomware, fileless malware, and living-off-the-land attacks don't always match known signatures. EDR catches the stuff that legacy antivirus misses — and gives your security team the tools to contain threats before they spread across your network.

What "Good" Looks Like

- Every company device — desktops, laptops, and servers — has EDR installed and actively monitored.
- Alerts are reviewed by real people (your IT team or a managed security provider), not just logged and ignored.
- The EDR solution can isolate a compromised device from the network in seconds.
- Your IT provider can show you threat reports and explain what's been detected and resolved.

Quick Self-Check

- [ ] All company endpoints have EDR (not just basic antivirus) installed
- [ ] Our EDR is actively monitored by our IT provider or a security operations center
- [ ] We receive regular reports on detected threats and how they were handled
- [ ] Our IT provider can remotely isolate compromised devices
- [ ] Personal devices used for work are also covered by our security tools
- [ ] Our EDR solution is kept up to date automatically

> *If your "antivirus" is something you bought at Best Buy five years ago, or if your IT provider can't explain what EDR solution they've deployed, you're running on hope — and hope is not a security strategy.*

03 EMAIL SECURITY

What It Is

Email security covers the tools and practices that protect your business from phishing, spoofing, malware-laden attachments, and business email compromise (BEC). It includes spam filtering, link scanning, attachment sandboxing, and authentication protocols like SPF, DKIM, and DMARC that prevent attackers from impersonating your domain.

Why It Matters

Over 90% of cyberattacks start with an email. Phishing is the single most common way attackers get into business systems. One click on a malicious link or one convincing fake invoice and an attacker can own your email, your files, or your bank account. Business email compromise alone cost organizations over $2.9 billion in 2023.

What "Good" Looks Like

- Advanced email filtering catches phishing attempts, malicious attachments, and spoofed sender addresses before they reach inboxes.
- SPF, DKIM, and DMARC records are properly configured for your domain, preventing attackers from sending emails that appear to come from your company.
- Suspicious links in emails are scanned in real time, and dangerous ones are blocked or rewritten.
- Your IT provider has configured policies to flag or block emails from external senders that impersonate internal employees.

Quick Self-Check

- [ ] We have advanced email filtering beyond basic spam protection
- [ ] SPF, DKIM, and DMARC are configured and enforced for our domain
- [ ] Malicious links in emails are scanned and blocked in real time
- [ ] Attachments are scanned or sandboxed before delivery
- [ ] External emails are labeled or flagged so employees can identify them
- [ ] We have policies to verify financial requests received via email (phone call confirmation, etc.)

> *The scariest attacks aren't the obvious spam emails with bad grammar. They're the ones that look exactly like a message from your CEO asking the accounting department to wire $50,000 to a "new vendor." If your email security can't catch those, you're exposed.*

04 BACKUP & DISASTER RECOVERY

What It Is

Backup and disaster recovery (BDR) is your safety net. Backups are copies of your data stored separately from your main systems. Disaster recovery is the plan and tooling to get your business back up and running when something goes catastrophically wrong — whether that's a ransomware attack, a hardware failure, a fire, or an act of nature.

Why It Matters

Ransomware can encrypt every file in your business in minutes. Hardware fails without warning. Natural disasters don't check your calendar. Without reliable, tested backups and a clear recovery plan, any of these events can put you out of business. 60% of small businesses that lose their data shut down within six months.

What "Good" Looks Like

- Your data is backed up at least daily, with critical data backed up more frequently.
- Backups follow the 3-2-1 rule: three copies of your data, on two different types of media, with one copy stored offsite or in the cloud.
- Backups are tested regularly — your IT provider can prove they can actually restore your data, not just that backups are running.
- You have a documented disaster recovery plan with defined recovery time objectives (RTO) and recovery point objectives (RPO).

Quick Self-Check

- [ ] All critical business data is backed up at least daily
- [ ] We follow the 3-2-1 backup rule (3 copies, 2 media types, 1 offsite)
- [ ] Backups are tested with actual restore drills on a regular schedule
- [ ] We have a documented disaster recovery plan
- [ ] Recovery time objectives (RTO) and recovery point objectives (RPO) are defined
- [ ] Backup alerts and failures are monitored and addressed immediately
- [ ] Backups are protected from ransomware (immutable or air-gapped copies)

> *"We have backups" is not the same as "we can recover." If your IT provider can't tell you exactly how long it would take to get your business back online after a total system failure — and prove it with a recent test — your backups might be worthless when you need them most.*

05 EMPLOYEE SECURITY AWARENESS TRAINING

What It Is

Security awareness training teaches your employees how to recognize and respond to cyber threats — phishing emails, social engineering, suspicious links, password hygiene, and safe data handling. It turns your biggest vulnerability (humans) into an informed first line of defense.

Why It Matters

Your employees are targeted every day. Phishing emails, fake login pages, phone scams, USB drops — attackers know that people are easier to hack than systems. No amount of technology can fully protect a business if employees don't know what to look for. One careless click can bypass every firewall and security tool you've invested in.

What "Good" Looks Like

- All employees complete security awareness training when they're hired and receive ongoing training at least quarterly.
- Training includes simulated phishing campaigns that test whether employees can spot real-world attacks.
- Results from phishing simulations are tracked, and employees who fall for them receive additional coaching (not punishment).
- Training covers current threats — not just generic slideware from 2018 — and is updated as the threat landscape changes.

Quick Self-Check

- [ ] All employees complete security awareness training during onboarding
- [ ] Training is conducted at least quarterly (not just once a year)
- [ ] We run simulated phishing campaigns to test employee awareness
- [ ] Phishing simulation results are tracked and reviewed
- [ ] Employees who fail simulations receive additional training
- [ ] Training content is updated regularly to reflect current threats

> *If your security training is a once-a-year PowerPoint that everyone clicks through while eating lunch, it's not training — it's a checkbox. Real training changes behavior. It should make your team genuinely better at spotting threats.*

06 INCIDENT RESPONSE PLANNING

What It Is

An incident response plan (IRP) is a documented, step-by-step playbook for what to do when a security incident occurs. It defines who does what, who to contact, how to contain the damage, how to communicate internally and externally, and how to recover. Think of it as your fire drill for cyberattacks.

Why It Matters

When a breach happens — and statistically, it will — panic is the enemy. Without a plan, people scramble, make mistakes, and waste critical time. A well-rehearsed incident response plan can mean the difference between a contained incident and a full-blown catastrophe. Companies with tested IRPs reduce the cost of a breach by an average of $2.66 million.

What "Good" Looks Like

- You have a written incident response plan that covers detection, containment, eradication, recovery, and post-incident review.
- Key roles and responsibilities are clearly defined — who leads the response, who handles communications, who contacts legal and insurance.
- The plan includes contact information for your IT provider, cyber insurance carrier, legal counsel, and law enforcement.
- Your team has practiced the plan through tabletop exercises at least once a year.

Quick Self-Check

- [ ] We have a written incident response plan
- [ ] The plan defines roles and responsibilities for key team members
- [ ] Contact information for IT, legal, insurance, and law enforcement is included
- [ ] The plan covers detection, containment, eradication, and recovery steps
- [ ] We have conducted a tabletop exercise or incident response drill in the past 12 months
- [ ] The plan is reviewed and updated at least annually

> *The worst time to figure out your incident response plan is during an actual incident. If you don't have one, you're gambling that you'll make perfect decisions under extreme pressure — and that's a bet you'll lose.*

07 NETWORK SEGMENTATION

What It Is

Network segmentation divides your business network into separate zones with controlled access between them. Instead of one flat network where everything can talk to everything, segmentation creates boundaries — so your guest Wi-Fi, your point-of-sale system, your file servers, and your security cameras each live in their own isolated segment.

Why It Matters

On a flat network, an attacker who compromises one device can move freely to every other device on the network. That means a single infected laptop can reach your financial systems, your customer database, and your backups. Segmentation limits the blast radius of an attack and makes it dramatically harder for threats to spread.

What "Good" Looks Like

- Your network is divided into logical segments — at minimum: internal corporate, guest/public, servers, and IoT/operational devices.
- Firewall rules control what traffic is allowed between segments, following the principle of least privilege.
- Guest Wi-Fi is completely isolated from your internal business network.
- IoT devices (cameras, printers, smart devices) are on their own segment, separate from workstations and servers.

Quick Self-Check

- ☐ Our network is segmented (not flat) with defined zones
- ☐ Guest Wi-Fi is isolated from the internal business network
- ☐ IoT devices are on a separate network segment
- ☐ Firewall rules restrict traffic between network segments
- ☐ Server and workstation segments are separated
- ☐ We review and update segmentation rules at least annually

> *If your guest Wi-Fi password gets your visitors on the same network as your accounting software, you have a problem. And if your IT provider set up your network as one flat VLAN and never revisited it — that's a conversation worth having today.*

Now What?

If you made it through all seven chapters and checked most of the boxes, congratulations — you're ahead of the vast majority of small businesses. Keep it up, and keep revisiting this checklist every quarter to make sure nothing has slipped.

If you found gaps — and most businesses do — don't panic. The goal isn't perfection overnight. The goal is progress. Pick the areas where you're most exposed and start there.

Here's a simple prioritization: if you don't have MFA everywhere, start there. It's the single highest-impact, lowest-cost security improvement you can make. Then make sure your backups are actually tested and your team is getting real security training. Everything else builds on that foundation.

And if you're looking at this list thinking "I have no idea where to start" or "I'm not sure my IT provider is handling any of this" — that's exactly why we wrote this playbook. You deserve to know where you stand.

Let's Talk About Your Security.

We offer a free, no-pressure cybersecurity assessment where we take an honest look at your current security posture and give you a clear, prioritized action plan. No scare tactics. No jargon. Just a straightforward conversation about what you need to protect your business.

Whether you have an IT provider who needs to step up, or you're looking for a partner who takes security seriously from day one — we're here to help.

GET YOUR FREE ASSESSMENT

flyght.support/contact

(419) 670-7100

support@flyght.support

7430 W Central Ave., Toledo, OH 43617