AT&T Business

Smart security, small business: A practical guide to reducing cyber risk

Create a cybersecurity plan that grows with your business

1 Arora, Rohit. "Four Things Small Businesses Fear This Halloween," Forbes, October 31, 2023.

Cyberattacks are getting smarter and small businesses are paying the price

Small businesses face disproportionate cyber risk compared to enterprise organizations

According to industry and government research, most cyber incidents at small businesses begin with common and often preventable entry points like human error and phishing emails.

In other words, hackers go after small businesses because they count on outdated systems, reused passwords, and slower response times.

That's the bad news. But there is some good.

As AI tools become more widely adopted, they're changing how businesses manage work and data. When enforced consistently, basic cybersecurity practices can dramatically reduce risk, and new technologies, like network-native tools, can elevate your network with protections that start sooner than those that are device-based or cloud security. This helps small businesses elevate networks to a security control plane.

In this guide, you will learn:

- **The threats most likely to target your business**
- **Where current tools may fall short**
- **How to simplify cybersecurity**
- **How to build a response plan and security-first culture**
- **How to strengthen your security posture in 30 days**
- **What to do when you need more expertise than your budget allows**
- **Resources for small business cybersecurity**

How bad actors access your network

Why simple mistakes can lead to serious breaches

Though cyberattacks have grown more sophisticated, bad actors continue to use time-tested methods to access business networks. Phishing, ransomware, stolen credentials, human error, website vulnerabilities, and cloud applications are the most common ways bad actors gain access to your small business network.

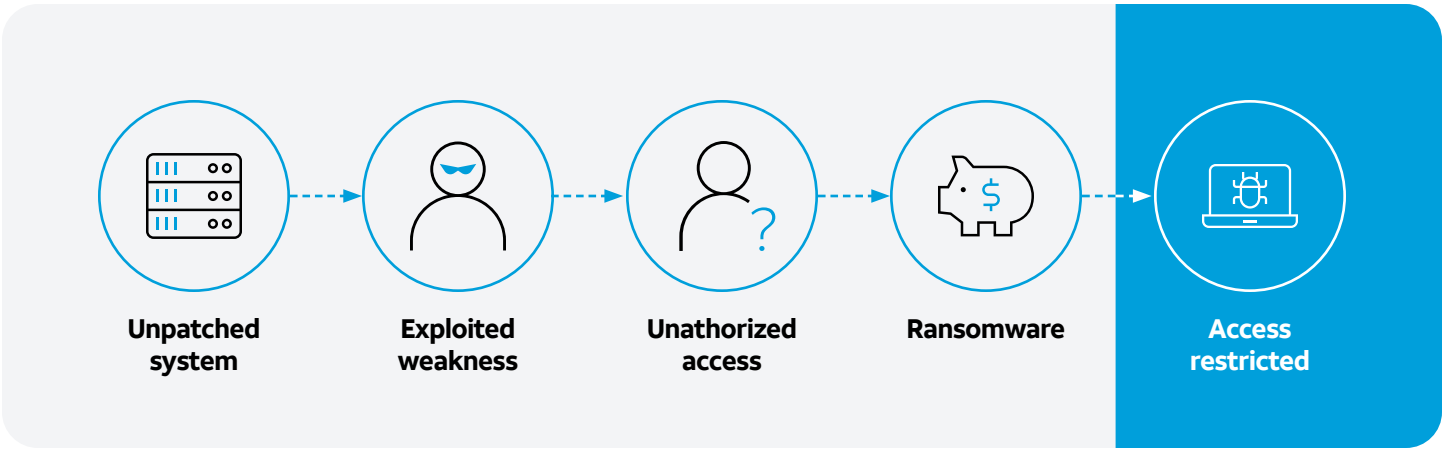
Phishing includes email links that install malware. And they are not always obvious. They could be fake communications from one of your vendors requesting payment details. Or phishing sites may look like the real ones to trick visitors into providing information like login credentials.

Phishing is also often the entry point for credential theft. Credential theft is the misuse of valid credentials by unauthorized users, and ransomware, which locks or encrypts your files. Attackers then demand a ransom in exchange for unlocking them.

Vulnerability exploitation happens when you delay updates or are unaware of system exposure. Attackers take advantage of unpatched software and misconfigured services to gain unauthorized access and, you guessed it, they deploy ransomware.

Whether it's a phishing email or an overlooked system exposure, the human element is the common denominator.

Now that you understand how these attacks work, the next step is finding ways to stop them before employees interact with them to reduce your risk.



Device-level protection isn't enough

Device-level tools matter, but are often not enough to stop modern attacks

Many small businesses trust device-reliant cyber protection products like antivirus software, email filters, and endpoint security tools.

These protective measures are important and useful elements of a cybersecurity strategy. But they typically only start protecting after a user clicks a link, downloads a file, or interacts with a website.

Although these solutions help protect your network, they often fall short against the threats most likely to affect small businesses, including phishing, ransomware, stolen credentials, human error, and known vulnerabilities. Starting cyber defense at the network level is more likely to stop threats before they reach a device.

When protection starts at the network

Blocking potential attacks sooner can reduce exposure to common attacks while reinforcing the security fundamentals you've already put in place.

Common threat	If protection happens only on devices	If protection happens at the network	Business impact
Phishing sites	Users can open malicious links before detection	Known phishing domains can be blocked before connection	Fewer successful credential theft attempts
Credential harvesting	Users may unknowingly enter passwords	Access to credential-stealing sites can be stopped	Reduced risk of account compromise
Ransomware delivery	Malware may download before security reacts	Known malicious infra-structure can be blocked	Lower chance of ransomware infection
Automated attacks	Systems are exposed to scanning and probing	Suspicious traffic can be interrupted earlier	Reduced exposure to automated threats
Human error	Security depends on users recognizing threats	Automatic filtering blocks known risks	Less reliance on perfect employee behavior

Strategy starts with simplifying cybersecurity

A strong cybersecurity strategy starts with the basics

You don't need to memorize frameworks and definitions to improve cybersecurity. A simple and practical approach is best, with a focus on the fundamentals that matter the most.

A successful small business cybersecurity strategy requires focus in five core areas:

1. **Know what you have**
   Identify the devices, systems, accounts, and data connected to your business. You can't protect what you don't know exists.

2. **Control who can access it**
   Reduce credential risk and limit unnecessary access to systems and data. One stolen password shouldn't open every door in your business.

3. **Protect everyday activity**
   Strengthen protection around email, browsing, and daily business workflows. Most attacks start with something that looked routine.

4. **Limit the blast radius**
   Contain threats so a single incident cannot spread across your business. A breach doesn't have to become a disaster.

5. **Recover quickly**
   Prepare your business to restore operations after a cyber incident. Getting back open fast is the goal.

Let's take a closer look at each of these core areas.

1. Know what you have

Identify what exists

How can you protect what you don't know exists?

Earlier, we went over how vulnerabilities like unpatched software can lead to unauthorized access to your network and often end in ransomware attack. This happens because devices, accounts, and systems were outdated, exposed, or just forgotten about without anyone realizing it.

Here are steps companies can take to reduce their risk.

- **List every device connected to your business network** This includes laptops, tablets, printers, routers, and any remote employee devices. Every connected device expands your exposure and should be accounted for.
- **Inventory all business accounts and cloud services** Document email systems, payroll platforms, file storage, CRMs, and vendor portals. Unused or forgotten accounts are often easy targets for attackers.
- **Identify who has administrative access** Admin accounts can change settings, access sensitive data, and control systems. Limit these privileges to only those who truly need them.
- **Remove what you no longer use** Retire outdated hardware, disable unused services, and close inactive accounts. Reducing complexity reduces risk.

AI tools: Keep your business safe

As Artificial Intelligence (AI) tools become more widely adopted, they're changing how businesses manage work and data. But small businesses need to be careful, because these tools can create safety problems.

The problem:

When workers put company files into AI tools online, that information leaves your business. Bad actors can see it. And customer details and money records should remain private.

AI tools help businesses work faster. They can sort information and handle tasks that take a long time. At the same time, attackers are using large language models and other tools to make deception more convincing. Phishing attempts that once raised red flags now can seem personalized and urgent for a response.

How to stay safe:

- **Check big requests.** If someone asks for money or sensitive info right away, ask them again in person or by phone. Don't use email alone.
- **Make simple rules.** Tell workers which AI tools they can use. Tell them what business information they can never share online.
- **Watch for danger.** Look for strange websites or connections on your internet.

The bottom line:

AI is powerful and helpful when used the right way. Good rules keep your business safe and smart.

2. Control who can access it

How to reduce credential risk deliberately

Teamwork may make the dream work, but it also lets threats in. When everyone has network access or when usernames and passwords are reused across multiple systems, bad actors get instant access to everything that runs your business as soon as one account is compromised. Remember about 1/3 of cyber incidents targeting small and midsized businesses use stolen or misused credentials.

- **Use strong, unique passwords for every account**
  Reused passwords allow attackers to move between systems quickly once one account is compromised. A password manager can simplify this process.
- **Enable multi-factor authentication (MFA)**
  MFA adds a second layer of verification, such as a code or device prompt. Even if a password is stolen, access can still be blocked.
- **Limit administrator privileges**
  Not every employee needs full system access. Restricting permissions reduces the damage if credentials are compromised.
- **Remove access immediately when roles change**
  Former employees or vendors should not retain active credentials. Timely updates prevent unnecessary exposure.

3. Protect everyday activity

Strengthen your daily defenses

Each time someone opens an email, clicks a link, or connects to your network your risk for intrusion and attack increases. And because these actions happen constantly throughout the day, attackers can disguise malicious activity in plain sight. Considering the ways you and your team get work done is important because daily internet activity is where many attacks begin.

- **Train employees to recognize suspicious messages**
  Urgent payment requests, unexpected login prompts, and unfamiliar links are common tactics. Knowing what to look for reduces accidental clicks.
- **Block known malicious websites before employees reach them**
  Some security approaches work at the network level, stopping access to harmful domains automatically. This reduces reliance on employees spotting every threat on their own.
- **Keep software and devices updated automatically**
  Updates fix known vulnerabilities that attackers actively exploit. Delays create opportunities.
- **Protect all connected devices, including remote workers**
  Home offices and mobile devices expand your network footprint. Security should extend wherever your business operates.

Build a safer workplace. Everyone can help.

Hackers trick people all the time. Your workplace can stay safer if everyone works together.

Here's what to do:

- Make simple rules about staying safe online
- Learn about cybersecurity throughout the year (free training is available online), not just once a year
- Tell your boss right away if you get a weird message or strange request
- Use two-way sign-ins for email and money accounts (this makes hacking much harder)
- Create strong passwords you don't reuse anywhere
- Use free and low-cost training resources available online from government, non-profit, and private entities like Cybersecurity and Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST) and their private partners

The good news:

Even small steps like learning the basics and two-way sign-ins can stop most attacks.

4. Limit the blast radius

Prepare to limit the damage of a breach

Limiting how far an attacker can move inside your environment is often the difference between a minor and major disruption. It's called limiting the blast radius, and it's less complicated than it sounds. Audit your configurations, close what you don't use and you've already limited how bad things can get.

- **Restrict shared folder, data access and separate critical systems**
  Segmenting critical systems and data and only granting access to employees or vendors that really need it reduces exposure and slows attacker movement in the event of a breach.
- **Monitor for unusual access behavior**
  Monitoring for unusual logins from unfamiliar locations at unexpected times may signal compromise. The earlier you spot the unusual behavior, the faster you can respond.
- **Reduce unnecessary external exposure**
  Fewer open doors equal fewer exploitation opportunities for attackers. Close the doors, get rid of unused remote access services, and audit your configurations.

5. Recover quickly

Build resilience in your operations

Larger organizations don't bet on being impervious and you shouldn't either. The ability to restore operations quickly after an attack is what makes the difference between a serious business interruption and a temporary disruption. When you prepare in advance, you can keep serving customers, keep taking orders, and keep cash flowing even when something goes wrong.

- **Maintain regular, automated backups**
  In high stress situations human-dependent processes may be more likely to fail. Make sure your backups can run without manual intervention.
- **Store backups separately from primary systems**
  To protect your paths to recovery, isolate your storage systems. This prevents ransomware from encrypting your backups.
- **Test restoration periodically**
  If it's not ready to go, it's not really a backup. Testing to ensure readiness is essential because a backup is only valuable if it works when you need it.

30 days to stronger cybersecurity

Small, practical steps reduce exposure

Understanding cyber risks is the first step. The next is making small, practical improvements that reduce exposure over time.

Even a basic plan that defines who is responsible for what, outlining what you should do next, and guidance on how to restore your operations can significantly reduce your business disruption and stress during an incident.

Without the direction a plan provides, confusion and delays can cause additional damage, costing you more money than the actual attack.

Stronger security for a smarter path to cybersecurity

Strengthen fundamentals for lasting security

Most small businesses don't need to implement dozens of security tools at once. In fact, meaningful improvements often come from focusing on a few core areas: knowing what systems you rely on, controlling who can access them, protecting everyday activity, limiting how far an attack can spread, and making sure you can recover quickly if something goes wrong.

- CISA Small business cybersecurity guidance
- NIST Small business cybersecurity corner
- FCC small business cyber planner 2.0
- AT&T cybersecurity insights

Turn your knowledge into action

Use the following checklist below to build stronger cybersecurity step by step.

Week 1: Know what you have

- ☐ List all devices connected to your business internet (computers, tablets, printers, POS systems).
- ☐ Inventory your most important business accounts and cloud services (email, payroll, file storage, CRM).
- ☐ Identify which users have administrator access.
- ☐ Remove inactive accounts or outdated systems that are no longer needed.

Week 2: Strengthen access controls

- ☐ Enable multi-factor authentication (MFA) for email, finance systems, and administrator accounts.
- ☐ Review password practices and avoid password reuse across systems.
- ☐ Limit administrator privileges to only those who truly need them.
- ☐ Remove system access for former employees or vendors.

Week 3: Reduce everyday exposure

- ☐ Turn on automatic updates for operating systems and applications.
- ☐ Train employees to recognize suspicious emails, urgent requests, or unfamiliar links.
- ☐ Review protections that block access to known malicious websites.
- ☐ Ensure remote devices connecting to your network are protected.

Week 4: Prepare to recover

- ☐ Verify that backups are running regularly.
- ☐ Test restoring at least one important file.
- ☐ Review who can access shared folders and sensitive data.
- ☐ Document simple steps to follow if a cyber incident occurs.

You shouldn't have to choose between running your business and protecting it.

AT&T Business connectivity solutions offer built-in security capabilities designed to help small businesses

Most small business owners didn't sign up to be IT managers. You're managing staff, serving customers, and watching cash flow. Cybersecurity is one more thing on a list that never gets shorter. That's the reality, and it's exactly why it shouldn't require a dedicated team or a separate budget line to stay protected.

AT&T Dynamic Defense® on AT&T Business Fiber builds protection directly into your internet connection, so threats are stopped at the network level before they ever reach your devices, your inbox, or your employees. Not after the fact. Not dependent on every device having the right software installed. Dynamic Defense on AT&T Business Fiber delivers the kind of threat intelligence, protection, and visibility that used to be reserved for companies with full security teams, to businesses just like yours.

Learn more about how **AT&T Dynamic Defense on AT&T Business Fiber** helps protect small businesses.

Why Dynamic Defense on AT&T Business Fiber?

Because protection shouldn't be a privilege. AT&T monitors over 1 trillion data flows every day across 1 exabyte of network traffic to deliver network-derived threat intelligence and network visibility that no device-level tool can. That intelligence powers Dynamic Defense on AT&T Business Fiber. When you combine the nation's largest fiber network with active threat protection built specifically for businesses like yours, you get enterprise-grade security without the enterprise overhead. The network is watching so you don't have to.

AT&T Business

AT&T Dynamic Defense is available with AT&T Business Fiber, AT&T Dedicated Internet, and AT&T Switched Ethernet on Demand with Internet Offload. Exclusions may apply.