SO,

You Think you Don't Need Cybersecurity



(A Business Owner's Guide to Avoid the Threats you can't see Coming!)

By Carmine J. Corridore; President
Underdog Cyber Defense

UNDERDOG
Cyber Defense

Table of Contents

- Page 2 -Why SMB's Think they don't need Cybersecurity(but do)
- Page 6 - Common Misconceptions
- Page 9 - What a secure business looks like
- Page 14 - Cyber Threats Don't Knock
- Page 17 - Five easy fixes to protect your business Today
- Page 21 - What is your Cyber IQ?

UNDERDOG
Cyber Defense



THE CYBERSECURITY BLIND SPOT

(Why Small Businesses Underestimate Cyber Threats—And Why That's a Problem)

Most business owners don't wake up thinking, *"I wonder if today is the day a cyberattack shuts me down."* But that's exactly why cybercriminals love targeting small and mid-sized businesses.

Cybersecurity isn't just for banks, hospitals, or Fortune 500 companies. If your business has emails, customer data, invoices, or an internet connection, you're a target. But many SMBs still believe:

- 🚫 "Hackers don't care about small businesses."
- 🚫 "I have antivirus software, so I'm fine."
- 🚫 "We don't store sensitive data, so there's nothing to steal."
- 🚫 "Cybersecurity is too expensive."

These false assumptions leave businesses vulnerable, and the worst part? Most owners don't realize it until it's too late.

UNDERDOG
Cyber Defense

43% of cyberattacks target small and mid-sized businesses.

A STORY THAT MIGHT SOUND FAMILIAR

The Manufacturer That Lost Everything Overnight

Jeff runs a small manufacturing company that supplies custom metal parts to auto dealerships and aerospace companies. His team relies on specialized CNC machines, and every order is tracked through a cloud-based inventory system.

One Monday morning, his team logged in and saw corrupted files everywhere. Customer invoices, production schedules, and CAD designs had been wiped out. The IT guy on staff checked their system—someone had accessed their cloud storage over the weekend and deleted everything

60% of SMBs that suffer a cyberattack close within 6 months.

UNDERDOG
Cyber Defense



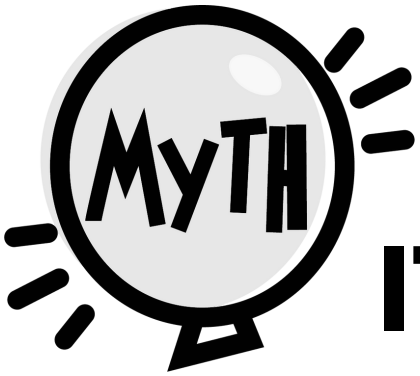
A former vendor's account had been compromised, and because they still had old login credentials, a hacker used it to slip in unnoticed.

Jeff had no offsite backups, so his entire operation was at a standstill. It took weeks to rebuild lost data and cost him thousands in missed deadlines and fines.

And all of this happened without a single hacker stepping foot in his factory.

Data breaches don't just cost money—they can trigger lawsuits, compliance fines, and lost

UNDERDOG
Cyber Defense



IT's Myth Busting Time

💀 "A Backdoor to Bigger Targets." Cybercriminals use SMBs as stepping stones—breaching your network to access your larger clients or vendors.

🚫 Myth #1: "We're Too Small to Be Hacked."

✅ The Truth: SMBs Are Cybercriminals' Favorite Targets.

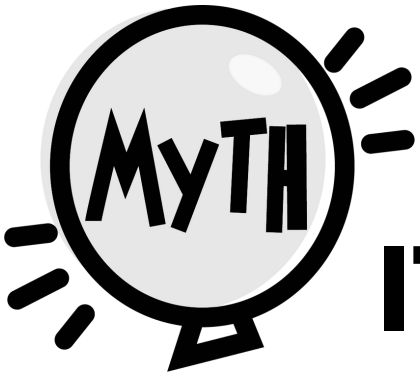
Many business owners believe hackers only go after big companies with deep pockets. The reality? 43% of cyberattacks specifically target small and mid-sized businesses—and most never recover.

🔹 Why? Because smaller companies usually have weaker security, outdated software, and fewer IT resources. Hackers know this, which makes SMBs an easier payday than trying to breach a Fortune 500 company.

🔹 Real-World Example: A small accounting firm in Texas was hit with an attack when an employee unknowingly clicked on a fake IRS email during tax season. The hacker gained access to client tax returns and financial records, then used them for identity theft and fraudulent tax filings. The firm faced lawsuits and lost major clients.

Small doesn't mean safe—it means vulnerable.

UNDERDOG
Cyber Defense



IT's Myth Busting Time

💀 "Easy Money." Hackers know small businesses don't invest in strong security, making them easy targets.

🚫 Myth #2: "We Have Antivirus, So We're Good."

✅ The Truth: Antivirus Alone Won't Stop Today's Attacks.

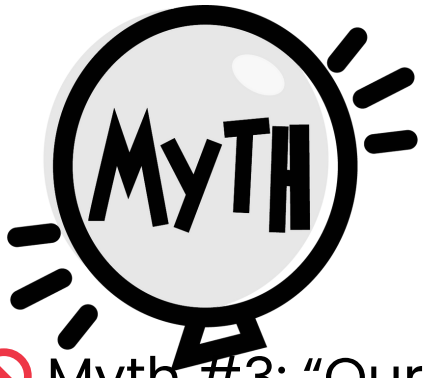
Antivirus software is only one layer of cybersecurity, and frankly, it's not enough. Cybercriminals today use phishing, social engineering, and credential theft—things antivirus programs can't detect.

🔹 Hackers don't just use viruses—they manipulate people. A simple fake email can trick an employee into handing over their login credentials—no virus needed.

🔹 Antivirus doesn't stop insider threats. If an employee accidentally gives a hacker access, your antivirus won't save you.

Think of antivirus like a seatbelt—it helps, but it won't stop a head-on collision.

UNDERDOG
Cyber Defense



IT's Myth Busting Time

🚫 Myth #3: "Our IT Guy Handles Security."

✅ The Truth: IT and Cybersecurity Are NOT the Same Thing. Many businesses assume their in-house IT person or outsourced IT provider is handling cybersecurity. But IT support and cybersecurity are two different specialties.

🔹 IT focuses on:

✅ Keeping computers, printers, and networks running.

✅ Setting up software and hardware.

✅ Troubleshooting tech problems.

🔹 Cybersecurity focuses on:

🚨 Detecting and preventing cyber threats.

🚨 Monitoring systems for suspicious activity.

🚨 Educating employees to prevent attacks.

💀 "A Quick Paycheck." Many SMBs panic and pay when attacked, especially if they don't have backups or an incident response plan.

UNDERDOG
Cyber Defense



What Real Cybersecurity Looks Like (And Why Your Business Needs It)

Spolier Alert

(Hint: It's More Than Just an Antivirus Subscription)

Most businesses think cybersecurity means having a firewall, running antivirus software, and telling employees not to click on suspicious emails. While those are pieces of the puzzle, they're not enough.

Real cybersecurity is about building a layered defense—like putting locks on your doors, installing an alarm system, and training your employees to recognize scams before they happen.

Here's what strong cybersecurity actually looks like in a modern business.

UNDERDOG
Cyber Defense



What Real Cybersecurity Looks Like (And Why Your Business Needs It)

Spolier Alert

(Hint: It's More Than Just an Antivirus Subscription)

🔐 1. Multi-Factor Authentication (MFA) – Your First Line of Defense

Imagine a thief trying to break into your office. If they steal a key, they're in. But if they also need a fingerprint scan or a code from your phone, it suddenly gets a lot harder. That's exactly how MFA works.

✅ What It Does: Requires users to enter a second form of verification (like a code from their phone) before logging in.

✅ Why It Matters: Over 80% of breaches happen due to stolen or weak passwords—MFA stops hackers even if they steal a password.

✅ Real-World Example: A CPA firm handling tax returns had a hacker attempt to log in using stolen employee passwords. MFA blocked the login attempt, preventing a data breach.

UNDERDOG
Cyber Defense



What Real Cybersecurity Looks Like (And Why Your Business Needs It)

Spolier Alert

(Hint: It's More Than Just an Antivirus Subscription)

📡 2. Network Monitoring & Threat Detection – Your Cyber Alarm System

You wouldn't leave your business unlocked at night without security cameras, so why do the same with your network? Hackers don't break in loudly—they sneak in and stay undetected.

✅ What It Does: Monitors your network 24/7 for unusual activity, alerting IT teams before hackers can do real damage.

✅ Why It Matters: Most breaches go undetected for months, giving hackers plenty of time to steal data.

UNDERDOG
Cyber Defense



What Real Cybersecurity Looks Like (And Why Your Business Needs It)

Spolier Alert

(Hint: It's More Than Just an Antivirus Subscription)

🛡️ 3. Employee Training – Because Your Team is Your Biggest Risk

Hackers don't break in—they log in. And they get in because employees accidentally let them in.

✅ What It Does: Teaches employees how to spot phishing emails, use strong passwords, and avoid social engineering attacks.

✅ Why It Matters: Over 90% of cyberattacks begin with a human error—training is the cheapest and most effective way to prevent them.

✅ Real-World Example: An auto dealership employee clicked on an email from a "vendor" asking for banking details. A quick-thinking finance manager recognized it as a scam, reported it, and stopped a $50,000 fraudulent wire transfer.

UNDERDOG
Cyber Defense



What Real Cybersecurity Looks Like (And Why Your Business Needs It)

Spolier Alert

(Hint: It's More Than Just an Antivirus Subscription)

🔍 4. Zero Trust Security – Don't Assume, Verify

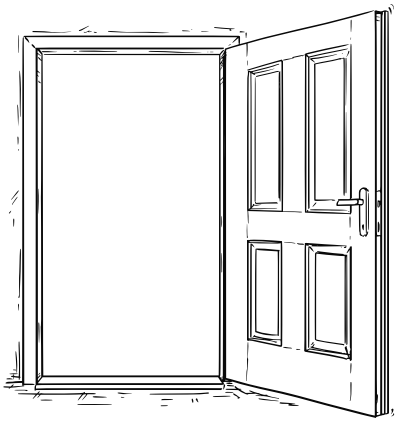
The old approach to security was "trust but verify"—today, it's "never trust, always verify." Hackers love when businesses assume "this user is safe" or "this device is fine."

✅ What It Does: Requires continuous verification—just because someone logged in this morning doesn't mean they should still have access.

✅ Why It Matters: Prevents hackers from moving through your system if they gain access to one account.

✅ Real-World Example: A financial firm used Zero Trust and caught a hacker posing as an employee, blocking them before they could steal sensitive financial records.

UNDERDOG
Cyber Defense



Cyber Threats Don't Knock: Are You Leaving the Door Wide Open?

(The Biggest Security Gaps Businesses Overlook —Until It's Too Late)

Most business owners assume cyberattacks are loud, obvious, and immediate—like a thief smashing a window. In reality, cybercriminals sneak in quietly, stay hidden for months, and strike when you least expect it.

The worst part? Most businesses don't even realize how exposed they are until the damage is done. Let's take a look at the most common ways hackers get in—and what happens when they do.

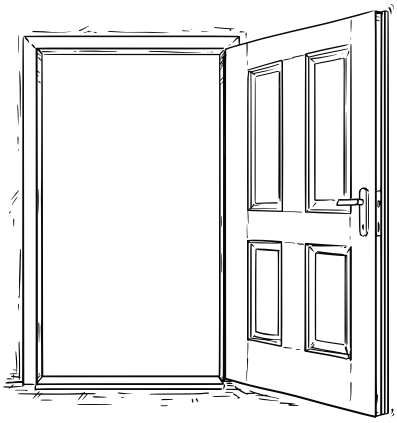
🚪 The Open Door: Unpatched Software & Outdated Systems

🔹 How Hackers Exploit It:

Old software and outdated systems are full of security holes that hackers know how to exploit. If you don't keep up with updates, you might as well leave your business's front door unlocked.

🔹 Fix It: Set up automatic updates for all software, operating systems, and applications. If a system can't be updated anymore, it's time to replace it.

UNDERDOG
Cyber Defense



Cyber Threats Don't Knock: Are You Leaving the Door Wide Open?

(The Biggest Security Gaps Businesses Overlook —Until It's Too Late)

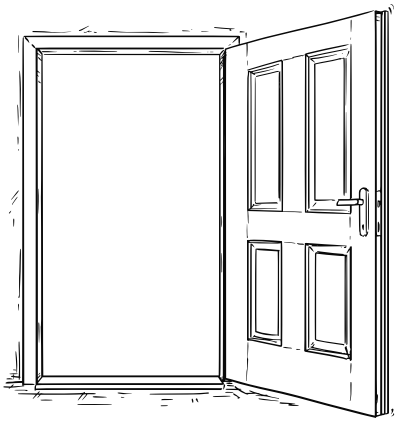
⚠ The Weak Link: Third-Party Vendor Access

- How Hackers Exploit It:

Businesses often share login credentials or connect their systems with outside vendors (accounting firms, payment processors, supply chain partners). If one of them gets hacked, the attacker can use their access to breach your company, too.

- Real-World Example: A regional manufacturing company worked with a third-party logistics firm to handle shipping. The logistics company's login credentials were compromised, giving hackers access to the manufacturer's inventory system. Orders were rerouted to fake warehouses, costing the company hundreds of thousands in lost products.
- Fix It: Limit vendor access to only what they need,

UNDERDOG
Cyber Defense



Cyber Threats Don't Knock: Are You Leaving the Door Wide Open?

(The Biggest Security Gaps Businesses Overlook —Until It's Too Late)

📧 The Disguised Threat: Business Email Compromise (BEC)

🔹 How Hackers Exploit It:

Hackers don't need to hack your network if they can trick your employees into handing over sensitive information. With Business Email Compromise (BEC), attackers impersonate a trusted person (like your CEO, accountant, or vendor) to convince employees to wire money, change payment details, or send sensitive data.

🔹 Fix It: Train employees to always verify payment requests by phone, set up email security filters, and use internal approval processes for large transactions.

🔹 Real-World Example: A small accounting firm received an email from what looked like a client requesting a bank transfer for a tax payment. The email looked identical to the real client's emails. The firm wired $85,000—only to realize the request was fake. The attacker had spoofed the email domain, making it appear legitimate.

UNDERDOG
Cyber Defense



From Sitting Duck to Cyber Secure: Five Easy Fixes to Protect Your Business Today

💻 1. Disable Unused Remote Access Tools (Because Hackers Love Open Backdoors)

🔹 The Problem: Many businesses set up remote desktop access (like RDP or TeamViewer) but never secure it properly. Hackers scan the internet for open remote access ports, break in, and steal or wipe your data.

🔹 Real-World Example: A small manufacturing supplier allowed remote access for an IT consultant but never disabled it after the project ended. Hackers found the exposed login portal, brute-forced the password, and gained full control of their network.

🔹 Quick Fix:

✅ Disable remote access for anyone who doesn't need it.

✅ Use a VPN or zero-trust security instead of exposing RDP to the internet.

✅ Require Multi-Factor Authentication (MFA) on all remote connections.

UNDERDOG
Cyber Defense



From Sitting Duck to Cyber Secure: Five Easy Fixes to Protect Your Business Today

🔌 2. Turn Off Bluetooth & Wi-Fi Auto-Connect on Company Devices (Because Cybercriminals Can Eavesdrop on You)

🔹 The Problem: Many business laptops, tablets, and smartphones automatically connect to public Wi-Fi and Bluetooth devices. Hackers use fake Wi-Fi hotspots and Bluetooth snooping to intercept sensitive data.

🔹 Real-World Example: A sales rep for an auto dealership worked remotely from a coffee shop. His laptop automatically connected to a fake "Free Wi-Fi" network set up by hackers, who captured his login credentials and later accessed the dealership's customer financing system.

🔹 Quick Fix:

✅ Disable automatic Wi-Fi and Bluetooth connections on all company devices.

✅ Use a mobile hotspot or VPN when working remotely.

✅ Implement Wi-Fi network security policies for employees.

UNDERDOG
Cyber Defense



From Sitting Duck to Cyber Secure: Five Easy Fixes to Protect Your Business Today

🛑 3. Block Personal Email & Cloud Apps on Work Devices (Because Employees Bring Their Own Security Risks)

🔹 The Problem: Employees log into personal email, Google Drive, or Dropbox on company computers, bypassing your security policies. If their personal accounts get hacked, attackers can use them to steal company data.

🔹 Real-World Example: A CPA firm employee used a personal email account to send work files home. The account was later compromised in a phishing attack, and hackers stole confidential tax documents. The firm faced client lawsuits and compliance penalties.

🔹 Quick Fix:

✅ Block access to personal email accounts on company devices.

✅ Require employees to use business-approved file-sharing platforms (like OneDrive or SharePoint).

✅ Implement Data Loss Prevention (DLP) rules to prevent sensitive data from leaving your network.

UNDERDOG
Cyber Defense



From Sitting Duck to Cyber Secure: Five Easy Fixes to Protect Your Business Today

📞 5. Create an Emergency Cyberattack Plan & Print It Out (Because When Systems Go Down, You Can't Google "What to Do")

🔹 The Problem: When a cyberattack happens, most businesses scramble to figure out what to do. If your email, phones, and internet are all down, how will your team communicate?

🔹 Quick Fix:

✅ Create a printed incident response plan with step-by-step instructions.

✅ Assign clear roles (Who contacts IT? Who alerts customers?).

✅ Include emergency contacts, backup procedures, and a plan for operating manually if needed.

Real-World Example: A regional logistics company was hit with a cyberattack that took down their entire network. With no backup plan, employees didn't know who to call, how to process shipments manually, or what to tell customers. They lost two weeks of revenue before recovering.

UNDERDOG
Cyber Defense



What's Your Cyber IQ?

Are You Playing It Safe or Playing with Fire?
Most business owners assume they have "decent" cybersecurity—until an attack proves otherwise. Let's put that confidence to the test. Answer these five quick questions to see if your business is cyber smart or cyber vulnerable.

1️⃣ Do you use Multi-Factor Authentication (MFA) on all critical accounts?

☐ A. Yes, we use MFA on email, financial systems, and key business applications.

☐ B. Only on a few important accounts.

☐ C. No, just strong passwords—MFA seems like overkill.

➡ Why It Matters: 80% of breaches happen due to stolen or weak passwords—MFA stops hackers even if they steal your login.

UNDERDOG
Cyber Defense



What's Your Cyber IQ?

2️⃣ If a key employee leaves, how quickly are their accounts shut down?

🔲 A. Immediately—access is removed as part of our offboarding process.

🔲 B. Within a few days, once IT gets around to it.

🔲 C. Honestly, I'm not sure if we revoke access at all.

➡️ Why It Matters: Former employees (or their compromised accounts) are a huge security risk. Hackers love old, forgotten logins that never get shut down.

UNDERDOG
Cyber Defense



What's Your Cyber IQ?

3️⃣ How do you and your team handle suspicious emails?

☐ A. We verify unexpected requests (especially financial ones) by calling the sender before taking action.

☐ B. We report phishing emails when we notice them, but not everyone is trained.

☐ C. We open emails if they look legitimate—who has time to double-check everything?

➡ Why It Matters: 91% of cyberattacks start with a phishing email—one wrong click can cost thousands.

UNDERDOG
Cyber Defense



What's Your Cyber IQ?

4️⃣ How often do you back up your business-critical data?

☐ A. Automatically, every day, with secure offsite storage.

☐ B. We back up data, but only every few weeks or when we remember.

☐ C. I think we have backups... somewhere.

➡ Why It Matters: Without recent backups, a cyberattack, hardware failure, or accidental deletion could wipe out your business overnight.

UNDERDOG
Cyber Defense



What's Your Cyber IQ?

5 If your business was hit by a cyberattack tomorrow, what would you do first?

☐ A. Follow our written incident response plan (which all key employees have a copy of).

☐ B. Call IT and hope they can fix it fast.

☐ C. Panic and Google "What to do after a cyberattack."

➡ Why It Matters: If you don't have a plan in place before an attack, you're already behind when disaster strikes.

UNDERDOG
Cyber Defense

Even one weak spot in your cybersecurity can lead to a major breach—but you don't have to fix it alone.

💡 Let's schedule a Free Cyber Risk Assessment to find out where your biggest security risks are—and how to lock them down before hackers find them first.

📞 Call Us: (570) 243-9205

📧 Email: hello@underdogcyber.com

🌐 Visit: www.underdogcyber.com

https://underdog.contact

UNDERDOG
Cyber Defense

SO,

You Think you Don't Need Cybersecurity



(A Business Owner's Guide to Avoid the Threats you can't see Coming!)

THANK YOU FOR READING

UNDERDOG
Cyber Defense