



The Security Reality Check

A concise assessment framework for business leaders who need clarity on their real security posture and its impact on enterprise growth.

Created by,

Vijaya Rao - Founder @Techvio | Cybersecurity Growth Partner for Mid-Size Enterprises



Before we dive into the assessment, here's why this matters — and why I'm the one guiding you through it.

I'm **Vijaya**, a cybersecurity and compliance strategist who has spent years helping mid-sized companies strengthen their security posture so they can unlock bigger markets, reduce deal friction, and accelerate enterprise sales.

Across dozens of organizations, I've seen one pattern repeat itself:

Most leaders believe their security is “good enough”... until buyers prove otherwise.

Security isn't just a risk issue anymore — it's a **revenue issue**.

And your ability to win enterprise trust depends on knowing exactly where your gaps are.

This quick assessment gives you that clarity.

If you run a **mid-sized business**, this wake-up call is for you.

Here's the reality: Nearly **46% of small and mid-sized businesses report experiencing a cyberattack**, and many struggle to recover — with several industry studies warning that a major breach can be financially devastating.”

But here's what nobody talks about—most business leaders have no idea where their security actually stands until it's too late.

This assessment gives you a clear picture of your real cybersecurity posture in under an hour, without the tech jargon or expensive consultants.

Today, You'll discover:

- Whether your business is a sitting duck or actually protected
- Which gaps could shut you down tomorrow
- What to fix first (hint: it's probably not what you think)
- How to turn security from a cost center into competitive advantage

The Real Numbers Every CEO Should Know

43% of all cyberattacks target small and mid-sized businesses, but here's the kicker:

29%

**Rate Their Defenses
as Adequate**

Small-to-medium
businesses with adequate
cyber defenses

\$187K

**Average Cost Per
Breach**

Typical financial impact
ranges from \$120K-\$254K

80%

No Formal Policy

Businesses without a formal
cybersecurity policy

14%

Highly Effective

Small businesses rating
their security as highly
effective

Translation: Most businesses are flying blind, and criminals know it.

Here's Your Immediate Security Assessment

Four quick checks that reveal everything



Check #1: The People Problem

Who actually owns security at your company?

Most breaches happen because nobody's really in charge. When something goes wrong, everyone assumes someone else will handle it.

01

Pick one person to be your "security point person"

02

Send an email to your team announcing who this person is

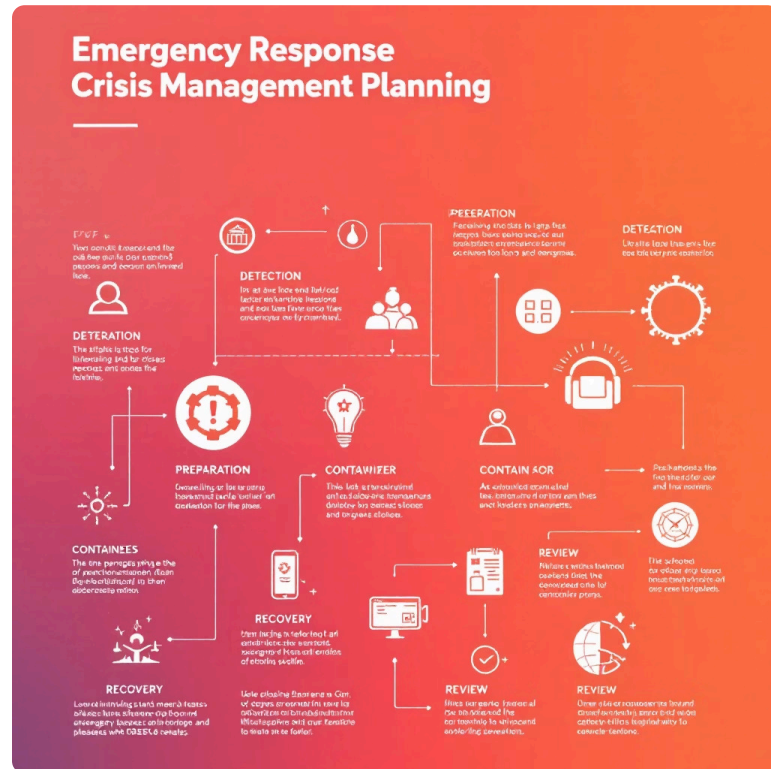
03

Give them permission to make security decisions

 **Why this matters:** Clear ownership = faster responses = less damage when (not if) something happens.

Check #2: The Process Reality

Question: What happens when things go wrong?



95% of breaches involve human error—not missing technology. The problem? Most companies wing it when crisis hits.

Take action right now:

- Open a document and write down who does what when you discover a breach
- Include: Who calls who? Who handles customers? Who contacts your insurance?
- Keep it simple—one page maximum
- Save it somewhere everyone can find it

Why this matters

Panic kills businesses. Plans save them.

Check #3: The Technology Truth

Question: Are your digital doors actually locked?

You probably have security tools, but are they actually protecting you? **80% of hacking incidents involve stolen passwords.**

→ **Text or call your IT person**

Ask if every employee has two-factor authentication on email

→ **Check endpoint protection**

Verify antivirus/endpoint protection is running on ALL devices (including phones/tablets used for work)

→ **Close the gaps**

If gaps exist, schedule time this week to close them

Why this matters

Criminals target the easiest path in. Don't be the easy target.

Check #4: The Governance Gap

Question: Who makes the final security decisions?

When your team wants to use a new app, hire a vendor, or give someone access to sensitive data—who decides if it's safe?



📌 **Why this matters:** Reactive decisions create holes. Proactive governance prevents them.

Now, what This Assessment Really Reveals

After completing these checks, you'll know:



If your business could survive an attack

Most can't—find out where you stand



Where criminals would likely get in

Usually not where you think



What your insurance actually covers

Spoiler: probably less than you assume



Whether your team knows what to do in a crisis

They probably don't

More importantly, you'll have immediate action items to fix the critical gaps without breaking the bank or drowning in complexity.



Ready to Go Beyond the Assessment?



If this assessment reveals gaps that make you uncomfortable (and it probably will), you don't have to fix them alone.

We help mid-sized business leaders build security programs that:

- Protect revenue and customer trust
- Pass insurance and compliance reviews
- Scale with your business growth
- Work without adding complexity or slowing you down

**No enterprise-grade
headaches**

No tool overload

**Just practical security that
fits your business**

Let's Talk About Your Real Security Picture

Book a free 30-minute conversation to:



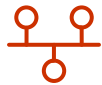
Review Your Results

Review your assessment results and discuss findings



Identify Blind Spots

Identify your biggest blind spots and vulnerabilities



Get a Roadmap

Get a realistic roadmap for improvement



Define "Good Enough"

Understand exactly what "good enough" looks like for your business

[Schedule Your Security Strategy Call →](#)

-
- ❏ P.S. - This isn't a sales pitch disguised as help. You'll walk away with specific, actionable steps whether we work together or not. But if you're serious about protecting what you've built, let's make sure you're not leaving the front door unlocked.