THE CYBERSECURITY EXECUTION GAP: A PRACTICAL GUIDE

For Mid-Market Manufacturing Companies

YOUR STEP-BY-STEP FRAMEWORK TO IMPROVE CYBER RESILIENCE WHILE GROWING FAST

Prepared by resourcive™

INTRODUCTION: WHY THIS GUIDE MATTERS

Mid-market manufacturers are growing fast, especially those backed by private equity and scaling through acquisitions. Even as IT teams push to keep up with operational growth, cybersecurity progress can lag behind, not from lack of awareness or effort, but because it's hard to execute in parallel with everything else.

The result? Gaps that increase your business to risk, regulatory pressure, and operational disruption.

From the factory floor to the finance office, the attack vector is increasing. Ransomware, supply chain attacks, and compliance failures don't just affect IT, they can halt production, erode trust, and cost millions.

This guide is designed to help manufacturing executives, especially CFOs and IT leaders, understand:

- Where the cybersecurity execution gap comes from
- How to assess the maturity of your current program
- What actionable steps to take next

You don't need another vendor selling tools. You need a roadmap that aligns security with business velocity.

SECTION 1

THE CYBERSECURITY EXECUTION GAP

What Causes the Gap:

No Dedicated Security Leadership

Most growing manufacturers don’t have a CISO. Security often rests on the shoulders of IT leaders who are highly capable but stretched thin. With limited bandwidth, tight budgets, and competing priorities, even clear risks can remain unaddressed — not for lack of skill, but lack of time.

Tool-First Thinking

The answer is never just buying another product. MSSPs sell managed detection, but they don't fix broken processes, clarify roles, or ensure alerts are actionable.

Lack of Execution Capacity

Knowing what to do isn’t enough. We frequently encounter open remediation items that persist, not because they’re ignored, but because day-to-day fires and competing demands leave no time to drive them across the finish line.

Disjointed Growth

Acquisitions mean new networks, new risks, and no time to standardize. We helped one firm uncover six separate antivirus tools across five sites — none centrally managed.

THE RESULT: Repeated audit findings, unclear risk exposure, wasted spend, and mounting risk — with no executive clarity on progress.

WHY MANUFACTURING IS ESPECIALLY VULNERABLE

- **Operational Technology (OT)** environments are harder to secure. Legacy systems can't be patched without disrupting production. Many facilities run outdated firmware or unsupported PLCs with flat network architectures. These gaps are invisible to traditional IT scans.

- **Supply Chain Pressure** is real. Customers are demanding cyber certifications to continue doing business. A supplier audit can become a crisis when controls can’t be evidenced.

- **Regulatory Scrutiny** is increasing. NIST, CMMC, and industry-specific standards are no longer optional.

- **Lean Teams** mean security responsibilities fall to the same people keeping email running and onboarding new hires. One manufacturer had a single IT manager responsible for six plants — with no time to drive security projects.

What this creates is a perfect storm: expanding attack surface, limited governance, and insufficient resources. And it's not a tech problem, it's a business risk problem.

DEFINING A PRACTICAL MATURITY PROGRAM

A practical maturity program is not another audit. It's a **way to operationalize security,** starting from where you are and moving toward where you need to be, without overengineering it.

What It Is:

A structured model for building a security program that aligns with business growth. This includes a maturity baseline, a prioritized action plan, and a system for tracking execution over time. You can use various dashboard tools to generate scoring, and task assignments, but it's the process that matters most.

Core Principles:

- **Execution-First:** Focus on getting traction, not creating binders. You need clarity on who does what, by when.
- **Risk-Based Alignment:** Tie cyber actions to business risk, downtime risk, and compliance exposure.
- **Minimal Internal Burden:** Design the process to work with available resources, not ideal ones.
- **Visibility:** Build or use a live dashboard to centralize maturity scores, task tracking, and owner accountability.

First Steps (2–3 weeks):

- Establish a maturity baseline using a practical framework (e.g., NIST CSF or CDM)
- Build a heatmap of risks, gaps, and compliance exposure
- Create a 90-day roadmap with assigned owners, sequencing, and measurable goals

The tools exist, but execution is what drives improvement.
If you're not tracking it, you're not progressing.

ACTIONABLE NEXT STEPS FOR MANUFACTURING LEADERS

1. **Start with a Whiteboarding Session**
   a. Bring IT, finance, and ops to the table. Cyber is everyone's problem.
   b. Map known risks, business dependencies, and current toolsets.
   c. Identify 1–3 high-impact initiatives you can act on now.

2. **Assess Organizational Ownership**
   a. Who is accountable for cyber outcomes today?
   b. Are acquired sites following the same standards?
   c. Are third parties (MSSPs, MSPs) operating under clear roles and KPIs?

3. **Review Existing Tools and Controls**
   a. Don't assume coverage equals protection. We've seen clients with EDR tools that weren't enabled on half their endpoints.
   b. Look for overlap and shelfware. Every dollar saved is a dollar that can be reinvested.

4. **Map to a Framework**
   a. You don't need gold-plated compliance. Use CDM or NIST to find your weakest links.
   b. Focus on Detect, Respond, and Recover — where manufacturers often score lowest.

5. **Define a 90-Day Sprint**
   a. Keep it lean: 3–5 prioritized projects.
   b. Assign owners. Define what success looks like. Track it.

6. **Build a Dashboard**
   a. Security needs a single source of truth.
   b. Use a platform to track posture, gaps, assignments, and progress.

WHAT GOOD LOOKS LIKE

When maturity programs are implemented with discipline:

- **Maturity gains of 1–2 levels** in priority domains are realistic in 6–12 months.
- **Risk exposure drops 30–50%** through measurable control deployment.
- **Tool spend becomes intentional,** with savings reinvested in higher-impact areas.
- **Executives and boards gain clarity,** not just compliance checklists.

This isn't about adding noise, it's about creating structure and traction with the resources you already have.

ABOUT THIS GUIDE

This guide is rooted in firsthand experience helping manufacturers mature their cybersecurity posture without losing operational momentum. We've seen what works, and what stalls.

You don't need a vendor to tell you security is important. What you need is a process for making progress.

Whether you run this process internally or want guidance and execution horsepower to get there faster, this guide gives you the framework.

- Establish ownership
- Identify waste
- Align action to risk
- Measure what matters

You can do this with the team you have. But if you need help, we're here.

WANT HELP PUTTING THIS INTO ACTION?

If you'd like expert guidance or execution support to accelerate your progress:

✉ Email us at **cyber@resourcive.com**

🌐 Or visit **resourcive.com/cyber-risk-security**

No sales pitch. Just help if you want it.