INTERMIXIT

FREE REPORT:
BUILT SPECIFICALLY FOR MANUFACTURING LEADERS

WARNING: The 7 Hidden IT Gaps That Could Bring Your Production to a Standstill

What Your IT Provider Isn't Telling You — And How Overlooked Gaps Could Put Your Production, Customers, and Uptime at Serious Risk!

Phone: 717-914-0102 | Email: hello@intermixit.com | Web: https://www.intermixit.com

INTERMIXIT

WARNING: The 7 Hidden IT Gaps That Could Bring Your Production to a Standstill

And Why Most IT Providers Miss Them Until It's Too Late

If you're in manufacturing, you already know: downtime isn't just expensive — it's disruptive. Every hour offline means missed deliveries, delayed jobs, and frustrated customers. You don't get the luxury of hitting pause. Your business runs on precision, and every moving part — from machines to systems to people — has to be dialed in.

That's why it surprises so many plant managers and business owners when the thing that takes them down isn't a broken machine or a supplier delay — it's a cyberattack.

Here's how it usually happens: an email comes in. It looks like an invoice. Seems routine. Someone clicks. Suddenly, your file server locks up, your ERP is down, your machines can't run, and no one knows what's happening.

No warning. No alerts. Just frozen screens and idle production lines.

We've seen it happen to well-run shops with solid teams and capable IT support. Not because they were careless — but because **most IT providers aren't built for manufacturing**. They know how to manage an office network. But segmenting legacy systems? Securing vendor remote access? Testing disaster recovery plans under real-world pressure? That's where things fall apart.

This report outlines the **7 most common IT gaps we uncover in manufacturing environments** — issues that are easy to miss, but brutal when they fail. These aren't hypothetical problems. They're the real-world blind spots that open the door to ransomware, data loss, and production downtime that ripples through your entire business.

Whether you've got an internal IT team, an outside provider, or some hybrid setup — this report will help you understand where risk hides, what your current setup might be missing, and what to do next.

Because protecting your uptime starts here — and it starts with visibility.

INTERMIXIT

What You'll Learn in This Report

This isn't a sales pitch, a compliance checklist, or a bunch of buzzwords. It's a behind-the-scenes look at the real IT risks hiding inside manufacturing operations — and how they lead to shutdowns.

Here's what you'll walk away with:

- The **7 most common IT gaps** we uncover during audits of manufacturing networks
- How to tell whether your current IT setup is actually protecting your production — or just reacting when things break
- The **hidden vulnerabilities** that ransomware groups target (and why they hit manufacturers so often)
- The **insurance requirements** that could deny your claim if you're not careful
- What a **resilient, factory-ready IT environment** looks like — and what steps to take next

If even one of these issues shows up in your systems, your production line could be one bad click away from a costly outage.

This report is here to help you catch it before that happens.

1. Your Backups Aren't Actually Recoverable

Most manufacturers assume their backups are working — until they need them. But when ransomware hits or a system fails, they find out the hard way: the backups were never tested, the data wasn't complete, or the recovery time is days, not hours.

If you haven't done a full test restore in the last 90 days, you're flying blind.

What to check: Are your backups isolated from your network (air-gapped)? How long would it take to restore full operations? Do you know who's responsible — and have they proven it works?

2. Your Network Isn't Properly Segmented

Flat networks are a gift to cybercriminals. If someone clicks the wrong email and malware lands on a workstation, a flat network lets it spread to your servers, backups, and even your production systems with no barriers.

Manufacturing networks should separate office systems, production equipment, and vendor access — but most don't.

What to check: Can your HVAC vendor reach your ERP? Can your office staff access your CNC machines? If the answer is yes, your entire operation is exposed.

3. Remote Access Is a Wide Open Door

Manufacturers often rely on remote access for vendors, technicians, and even internal users. But in too many cases, that access is poorly controlled — using outdated VPNs, shared logins, or no multi-factor authentication (MFA).

These are prime entry points for ransomware groups. One leaked credential can open the door to everything.

What to check: Who has remote access, and how is it secured? Are old accounts still active? Is MFA enforced everywhere? If not, you're vulnerable.

4. You're Using IT That Was Built for Offices — Not the Factory Floor

Most IT providers are great at supporting office environments: file sharing, email, Microsoft 365, basic firewalls. But manufacturing operations come with a different set of demands — like legacy machines that can't be patched, production systems that can't go offline, and vendor access that needs tighter controls.

The problem isn't that your IT team is bad. It's that they're often applying a one-size-fits-all approach to a setup that's anything but typical.

What to check: Has your IT provider taken the time to understand how your production environment works? Do they know what systems are most critical to uptime? Can they explain how they'd isolate a breach without shutting down operations?

5. Users Aren't Trained to Spot ThreatsPhoine

Your people are your first line of defense — and often the weakest. Phishing emails are getting harder to spot, and most manufacturers don't provide regular training or testing.

Even one untrained user clicking a fake invoice can take down your entire operation.

What to check: When was the last time your team got cybersecurity training? Do you simulate phishing attacks? If not, they're being targeted — and probably not ready.

6. There's No Clear Plan for What Happens If Things Go Wrong

When a cyberattack hits, the last thing you want is confusion. But that's exactly what happens in most businesses — even ones with solid IT support. People aren't sure who to call, what systems to shut down, or how to keep things moving.

Having a written, tested response plan can be the difference between a quick recovery and a days-long shutdown.

Too often, "the plan" lives in someone's head… or worse, doesn't exist at all.

What to check: If ransomware hit tomorrow, who's doing what — and how quickly? Is there a documented plan everyone knows? Has it ever been tested with your team, not just your IT provider?

7. Your Cyber Insurance May Not Cover What You Think It Does

A lot of manufacturers assume their insurance will kick in if something bad happens. But over the past year, we've seen a sharp rise in denied claims — and it's not always because the business was negligent. It's because the provider didn't meet certain baseline protections… and didn't know it.

Things like MFA, documented policies, secure backups, and basic logging are now table stakes — and if you can't show proof, you might be on your own after an incident.

What to check: Have you reviewed your policy recently? Do you know what controls are required to stay compliant — and are you sure your current setup meets them? Cyber insurance is evolving fast, and many policies quietly shifted the rules.

You've Seen the Gaps—Now What?

If you've read this far, chances are something hit close to home. Maybe a few of these gaps look familiar. Maybe your gut's been telling you for a while that your current IT setup isn't as locked down as it should be.

You wouldn't ignore a mechanical issue on your floor. This isn't any different.

Good Shops Get Caught Off Guard All the Time

Here's the problem: most firms don't realize there's an issue until something breaks. A ransomware attack. A failed backup. A compliance fine. That's when panic sets in—and the finger-pointing starts.

But by then, it's too late to prevent it.

The good news is that you don't have to wait for the disaster. **You can get ahead of it.**

Real Confidence Starts with Clarity

This report wasn't about scare tactics. It's about giving you a clear view of what's under the hood. Because once you can see the weak points, you can do something about them.

The manufacturers who come out ahead aren't just the ones with the newest equipment — they're the ones who know how to protect what keeps them running. They ask the right questions. They fix problems before they become downtime. And they treat IT the same way they treat safety and quality: as mission-critical.

So What's the Next Step?

It's not about ripping everything out or replacing your current provider tomorrow. You don't need a massive overhaul to start fixing the problem. What you do need is clarity — a clear-eyed look at where things stand today, where the vulnerabilities are hiding, and how exposed your production really is if something goes wrong.

Because in manufacturing, it's rarely one big mistake that causes a shutdown — it's a chain reaction from one small gap that no one saw coming.

This is your chance to catch it now… before it catches you.

We've made that first step simple….

How to Get Started with IntermixIT

1. **Book Your 15-Minute Introduction Call – www.intermixit.com/15minutes**
   This isn't a sales pitch. It's a focused conversation to get familiar with your current setup, what challenges you're facing, and where downtime or security issues are keeping you up at night. We'll also walk you through how our no-cost cybersecurity assessment works — and what you can expect to learn.

2. **Get Your Cybersecurity Assessment**
   Our team will conduct a practical, high-impact review of your IT environment — with a manufacturing lens. That means looking at the systems that keep your operations moving: network design, backups, remote access, user risk, and more. No fluff, no jargon. Just clear insights you can act on.

3. **Review Your Results and Explore Your Options**
   We'll walk you through the findings, answer your questions, and show you exactly how IntermixIT could help strengthen your defenses and support your uptime. Whether you work with us or not, you'll walk away with a better understanding of where you stand — and what needs attention.

Get Started with IntermixIT – A 15-Minute Call to Secure Your Assessment
Schedule Here - *www.intermixit.com/15minutes*

Want to See How Other Companies Are Locking Down IT With IntermixIT?

While every industry is different, the risks of poor IT are universal. Visit our case study library to see how IntermixIT helps companies improve uptime, security, and confidence — and how we could do the same for you.

Scan the Code - Read the Case Studies!

https://intermixit.com/success-stories/

Take a look inside these success to see how IntermixIT can provide the secure, reliable IT support your company needs.