# MFG MINDS

**EDITION 01 · 23-OCTOBER-2026 · WHERE SHOULD YOUR ERP LIVE?**

*Insights for manufacturing leaders, from Expandx*

Namaskar, Manufacturing & Supply Chain Leaders,

Here is a number worth pausing on: the world's 500 largest companies lose about **$1.4 trillion a year to unplanned downtime**, roughly **11% of their revenue**.[1] A single idle line at a major automotive plant can cost **up to $2.3 million an hour**, around ₹20 crore.[1]

Few plant heads connect that to one quiet decision taken years ago: **where their ERP actually lives**. On a server in the plant? In a private cloud? On public cloud? It looks like an IT question. In practice, it decides your uptime, your exposure to cyberattacks, and what you really pay over five years.

At Expandx we have watched this choice play out across 100+ manufacturers. Here are three myths we hear most often, and the facts that break them.

FIRST, THE BASICS

## Three ways to run your ERP

| Model | What it is | Biggest strength | What you take on |
|---|---|---|---|
| **On-premise** | Servers in your own plant or office | Full physical control | You own hardware, power, backups, patching and IT staff |
| **Private cloud** | A dedicated environment for you in a professional data centre | Control of on-prem, without running the hardware | Costs more than shared public cloud |
| **Public cloud** | Shared infrastructure from a large provider | Fastest to start; scales instantly | Less room to tailor the environment; you still own access and passwords |

There is no universally "best" option, only the right fit for your scale, connectivity and risk appetite.

MYTH 1

## "Our server is inside our plant, so our data is safe."

**27.7%**

THE FACT

of all cyberattacks worldwide in 2025 hit **manufacturing**, the most attacked industry for the **fifth year running**. **68%** of those incidents were in **Asia-Pacific**.[2]

Attackers are not after your drawings. They are after your downtime, because a stopped plant pays fast. In a 2025 survey of 332 manufacturers, the top way in was an **unpatched, known vulnerability (32%)**. The biggest organisational gap was **lack of in-house security expertise (42.5%)**.[3]

**What it means for your plant:** a server in the plant cabin, patched "when someone gets time", behind a shared admin password, is exactly what attackers look for. Physical closeness is not security; disciplined operation is.

MYTH 2

## "Downtime is an IT problem."

**> 50%**

THE FACT

of major outages are caused by **power problems**, with **UPS failure** the most common culprit. **Human error** plays a part in roughly **two-thirds to four-fifths** of them.[4]

Those numbers come from professional data centres with redundant power and trained staff. The average large plant still loses **27 hours a month** to unplanned downtime.[1]

**What it means for your plant:** if the experts are tripped up by power and people, a plant with voltage fluctuations, a single UPS and a part-time IT person is far more exposed. When the ERP is down at month-end, dispatch stops, invoices stop, and that is a business problem.

MYTH 3

## "Cloud is automatically safer and cheaper."

**99%**

THE FACT

of cloud security failures, Gartner predicted, would be **the customer's fault**, not the provider's, through 2025.[5]

The cloud provider secures the hardware, power and building. **Your users, passwords and access rights are still your job.** And for a stable, predictable workload, a dedicated private cloud can cost less over five years than pay-as-you-go public cloud.

**What it means for your plant:** do not choose on the first-year invoice. Compare the **5-year total cost of ownership**, and get a clear answer to "who is responsible for what" in writing.

THE ONE QUESTION FOR THIS FRIDAY

## When did you last restore your ERP backup, not just take one?

**93%**

of cyberattacks go after the **backup storage** itself[6]

**39%**

of attacked organisations **lost their backups completely**[6]

**51%**

of hit manufacturers **paid the ransom** to get data back[3]

A backup that has never been restored is a hope, not a plan. Ask your team or your vendor for one test restore this month, and time how long it takes.

TAKE IT TO YOUR NEXT REVIEW

## 5 questions to ask about where your ERP lives

1. Is our data stored in India, and can we name the data centre?

2. How often is it backed up, is a copy kept offsite and offline, and when was a restore last tested?
3. If the system goes down, how many hours until we are running again, and is that written in our agreement?
4. Who applies security patches, and within how many days of release?
5. If we ever leave, can we export all our data in a usable format, and at what cost?

The attached PDF carries a detailed commentary on this topic, for your next management review or to share with your IT team.

If you would like a quick, no-obligation view of whether your current setup still fits your growth plans, **just reply to this email**. We will walk you through it.

Warm regards,

**Aditya Achlerkar**
Founder, Director, Expandx Solutions Pvt. Ltd.
IIT Delhi Manufacturing

**Sameer Dhamangaonkar**
Co-Founder, Director, Expandx Solutions Pvt. Ltd.
SPJIMR, NLSIU, Stanford Seed

Manufacturing & Supply Chain SaaS · tejoerp.com · expandx.in

**SOURCES**

[1] Siemens, The True Cost of Downtime 2024 (summary by AEMT). https://www.theaemt.com/resource/the-true-cost-of-downtime-2024-a-comprehensive-analysis.html

[2] IBM X-Force Threat Intelligence Index, via Manufacturing Dive (Feb 2026). https://www.manufacturingdive.com/news/manufacturing-sector-saw-most-cyberattacks-in-2025-IBM-X-Force/813063/

[3] Sophos, The State of Ransomware in Manufacturing and Production 2025. https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-manufacturing-and-production-2025

[4] Uptime Institute Annual Outage Analysis 2025, via The Register. https://www.theregister.com/2025/05/07/human_error_a_factor_in

[5] Gartner prediction, cited in CSO Online: The shared responsibility model explained. https://www.csoonline.com/article/570779/the-shared-responsibility-model-explained-and-what-it-means-for-cloud-security.html

[6] Veeam 2023 Ransomware Trends Report (press release). https://www.veeam.com/company/press-release/new-veeam-research-finds-93-percent-of-cyber-attacks-target-backup-storage-to-force-ransom-payment.html

Rupee figure converted at an approximate exchange rate. Figures are from the cited third-party reports; Expandx has not independently audited them.

You are receiving this as a valued Expandx associate. To stop receiving MFG Minds, reply with “unsubscribe”.