

CUSTOMER SUCCESS STORY

Production restarted in hours, not weeks.

A manufacturer treated ransomware as an IT risk until a peer lost eleven production days. **UPC Cyber vault** reframed it as an output risk — and put a clean, validated copy behind every line-critical system.

Per hour of downtime

In manufacturing, recovery time converts directly into lost output. A production line that cannot restart is a fixed cost running against zero throughput, and the difference between a four-hour and a four-day recovery is measured on the P&L rather than in a service report.

THE SITUATION

OT protected by assumption

Production planning, MES integration, and quality systems were backed up. Beyond that, little was certain:

- **OT and IT backups shared infrastructure.** A compromise of the corporate estate reached the systems running the plants.
- **Restore had never been attempted at plant scale.** Individual file restores worked; a full line restart was untested.
- **Legacy control systems were excluded.** Older platforms fell outside the standard backup scope.
- **Ransomware detection was perimeter-based,** offering nothing once an intruder was already inside.

THE DECISION

Protect the line, then rehearse the restart

The manufacturer put line-critical systems into an immutable, air-gapped vault with AI ransomware detection, then rehearsed a full plant restart from vault copies.

“Finance understood it the moment we costed a week of stopped lines. Before that it was an IT budget item. After that it was insurance on output.”

— VP, MANUFACTURING IT

DEPLOYMENT SNAPSHOT

SECTOR

Multi-plant discrete manufacturer

PROTECTED

Production planning · MES · Quality · Legacy control

STORAGE

Immutable WORM object storage

ISOLATION

Air-gapped from the corporate estate

DETECTION

AI ransomware detection on encryption patterns

RECOVERY

Multi-VM instant recovery per plant

REHEARSAL

Full plant-restart exercise from vault

COVERAGE

Legacy platforms included

WHAT WAS DEPLOYED

Immutability

Line-critical system images and configuration held as **WORM copies**, protected from deletion or encryption within retention.

Isolation

The vault is **air-gapped from the corporate estate**, so a compromise that reaches IT does not reach the recovery copies for OT.

Detection

AI ransomware detection spotting encryption patterns in real time, so an attack in progress is identified rather than discovered at shift change.

Recovery

Multi-VM instant recovery restoring a plant's systems as a group, rehearsed against the sequence a real restart requires.

WHAT CHANGED

BEFORE UPC CYBER VAULT

- OT and IT backups sharing **the same infrastructure**
- Full plant restart never attempted from backup
- Legacy control systems outside backup scope
- Detection limited to the perimeter
- Recovery time unknown, so downtime cost unmodelled

WITH UPC CYBER VAULT

- Line-critical copies **air-gapped** from corporate IT
- A **rehearsed plant restart** with a measured time
- Legacy platforms inside the protection scope
- **AI detection** of encryption behaviour in progress
- Downtime exposure quantified for the board

WHERE THE CHANGE CAME FROM

Output, not uptime

Expressing recovery time as lost production rather than service availability is what moved the decision from an IT budget to a business one.

Rehearsal found the sequence

A full restart exercise surfaced dependency and licensing issues that no file-level restore test would ever have revealed.

Legacy stopped being an exception

Including older control platforms closed the gap that would otherwise have determined the actual recovery time.

WHY THIS MATTERS IN MANUFACTURING

Capabilities doing the work in this deployment:

Air-gapped OT protection

Immutable WORM copies

AI ransomware detection

Multi-VM plant recovery

Rehearsed restart

Legacy platform coverage

Measured recovery time

Quantified downtime risk

BOTTOM LINE

UPC Cyber vault turned an untested backup into a rehearsed plant restart, with clean copies an attacker in IT cannot touch.

Ready to test **your last clean copy?**

Book a Cyber vault architecture review, or run a ransomware recovery simulation.

UPC Cyber vault

UNITEDLAYER.COM



EMAIL

contact@unitedlayer.com



PHONE

[+1-888-853-7733](tel:+1-888-853-7733)



X

x.com/unitedlayer



LINKEDIN

linkedin.com/company/unitedlayer