URVARA RANSOMWARE READINESS CASE STUDY

The Problem: A manufacturing company with 400 employees got hit by ransomware attack:

- Production systems locked for 11 days
- $2M ransom demand
- Backups were also encrypted (attacker had access for 3 weeks)
- Lost $4M in production downtime
- No incident response plan

Our Solution:

- Offline immutable backups (can't be encrypted)
- Network segmentation (isolate critical systems)
- Endpoint Detection & Response on all company devices
- Ransomware simulation & incident response drills
- Constant threat monitoring

Results - after 6 months:

- Survived 2 ransomware attempts (detected & blocked within minutes)
- Recovery time reduced from 11 days to 6 hours
- Zero production downtime from cyber attacks
- Cyber insurance premium reduced by 35%
- Employee security awareness increased 80%
- Avoided in potential downtime, saved annually on insurance

Notes: Better to be prepared if the worst case actually happens. Offline backups with rapid detection is key for business survival. With URVARA’s ransomware readiness solutions, be prepared for everything.