

LIYATECH EXECUTIVE READINESS SERIES

INDUSTRIAL, INFRASTRUCTURE & OPERATIONS CYBER READINESS CHECKLIST

Mining, Manufacturing, Construction, Engineering, Logistics, Energy & Utilities, Aviation

“If your operational systems were disrupted today, how quickly would production, logistics, or services stop?”

Introduction

Industrial and infrastructure-based organisations depend on continuous operations.

Production lines, control systems, logistics platforms, and operational technology environments are the backbone of performance, safety, and delivery.

Unlike office-based environments, even short disruptions can lead to:

- Production downtime
- Safety risks
- Supply chain delays
- Financial losses
- Operational instability

This checklist is designed to help leadership teams assess whether their organisation is truly prepared for cyber risks that directly impact operational continuity.

Tick what applies to your organisation.

1. Operational Technology (OT) & Production Systems

- ☐ We have full visibility of all operational technology (OT) and production systems across our environment.
 - ☐ Critical production or operational systems are isolated or protected from general business networks where necessary.
 - ☐ We understand which systems would cause production shutdown if compromised.
 - ☐ We regularly assess security risks across industrial control or operational systems.
-

2. Production Continuity & Downtime Risk

- ☐ We are confident we could maintain or restore production if key systems were disrupted.
 - ☐ We know how long it would take to resume operations after a major system failure or cyber incident.
 - ☐ We have identified the operational processes that are most critical to business continuity.
 - ☐ Downtime scenarios (including cyber incidents) have been tested or simulated.
-

3. Ransomware & Operational Disruption

- ☐ We understand how ransomware could impact production systems, not just office IT systems.
 - ☐ We have systems in place to detect ransomware activity early in both IT and operational environments.
 - ☐ Backup systems are protected from being encrypted or disabled during an attack.
 - ☐ We are confident we could recover operations without paying ransom in a worst-case scenario.
-

4. Third-Party & Remote Access Risk

- ☐ Contractors, vendors, and service providers access operational systems in a controlled and monitored way.

- ☐ Remote access into operational environments is secured and restricted.
 - ☐ We know exactly which third parties have access to our systems at any time.
 - ☐ Third-party access is reviewed regularly to reduce unnecessary exposure.
-

5. Industrial Cybersecurity & System Integrity

- ☐ We can detect unauthorized changes to operational systems or configurations.
 - ☐ Critical systems are monitored for abnormal behaviour or unexpected activity.
 - ☐ We have controls in place to prevent accidental or malicious changes to production environments.
 - ☐ We understand the cyber risks associated with legacy industrial systems.
-

6. Incident Response & Recovery Readiness

- ☐ We have a clear response plan for cyber incidents affecting operational systems.
 - ☐ Key operational and IT teams know their roles during a disruption event.
 - ☐ Recovery procedures are documented and tested.
 - ☐ We are confident we could coordinate IT and operational teams during a cyber incident.
-

Leadership Reflection

This checklist is designed to highlight operational exposure — not to provide a score.

If several responses were **“No” or “Not Sure”**, it may indicate risk in areas affecting:

- Production continuity
- Safety and operational control
- Supply chain stability
- Financial performance

- System integrity
 - Recovery capability
-

Optional Executive Conversation

If this checklist raised questions about your operational resilience or cybersecurity posture, a structured discussion can help clarify where your biggest risks sit and what practical steps can reduce exposure.

Contact

Nomfundo Makapela

 nomfundo.makapela@liyatech.co.za

 073 582 4195

Terence Moabi

 terence.moabi@liyatech.co.za

 078 710 4180

 www.liyatech.co.za