ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Oil Companies: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

VISIBILITY

01 ☐ Do we have a complete, current inventory of every OT asset, including firmware versions?

02 ☐ Do we know every connection between our IT and OT networks?

03 ☐ Do we know which vendors can access our sites remotely, and how?

ACCESS

04 ☐ Is multi-factor authentication enforced on all remote access, including old VPN accounts?

05 ☐ Are dormant accounts and former employees' accounts disabled promptly?

06 ☐ Are privileged and engineering accounts separate from everyday accounts?

NETWORK

07 ☐ Is there a DMZ between IT and OT, with no direct traffic crossing it?

08 ☐ Are safety instrumented systems isolated from the rest of the control network?

09 ☐ Are links to remote sites and offshore facilities encrypted and monitored?

DETECTION

10 ☐ Do we monitor OT network traffic, not just IT?

11 ☐ Would we notice a change to PLC logic or a safety system setting?

12 ☐ Are logs kept long enough to investigate an intrusion that started months ago?

RESILIENCE

13 ☐ Are backups of critical systems, including control logic and configurations, stored offline and tested?

14 ☐ Can we run key processes manually if IT systems are down?

15 ☐ Do we have spare hardware for critical controllers and HMIs?

RESPONSE

16 ☐ Do we have an incident response plan that covers both IT and OT?

17 ☐ Have we decided in advance who can order an operational shutdown?

18 ☐ Have we run a tabletop exercise in the last 12 months that included operations staff?

PEOPLE AND GOVERNANCE

19 ☐ Have field staff and contractors been trained on phishing and removable media risks?

20 ☐ Does the board receive regular reporting on OT cyber risk?