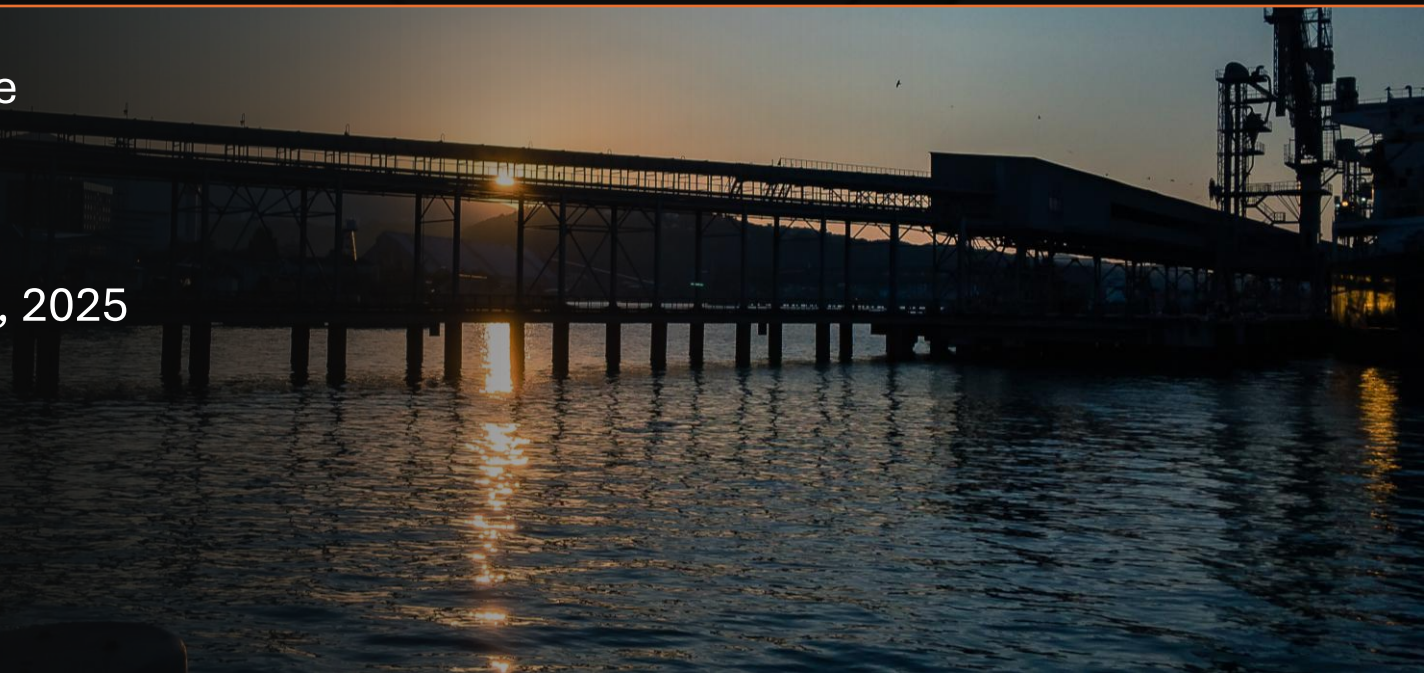


"Ports, Packets, and Pressure: Securing Bulk Terminals in a High-Threat World"

Richard Hodder - Managing Director, Engage
Cyber

ABTO Bulk Terminals Conference, Marseille, 2025



The 3 AM Call

- Night shift, ship half-loaded
- Screens freeze, conveyors stop
- Engineer plugs in laptop → network crash
- 48 hours downtime → €600,000 loss



“Cyber starts as an inconvenience — but it ends as a balance-sheet problem.”

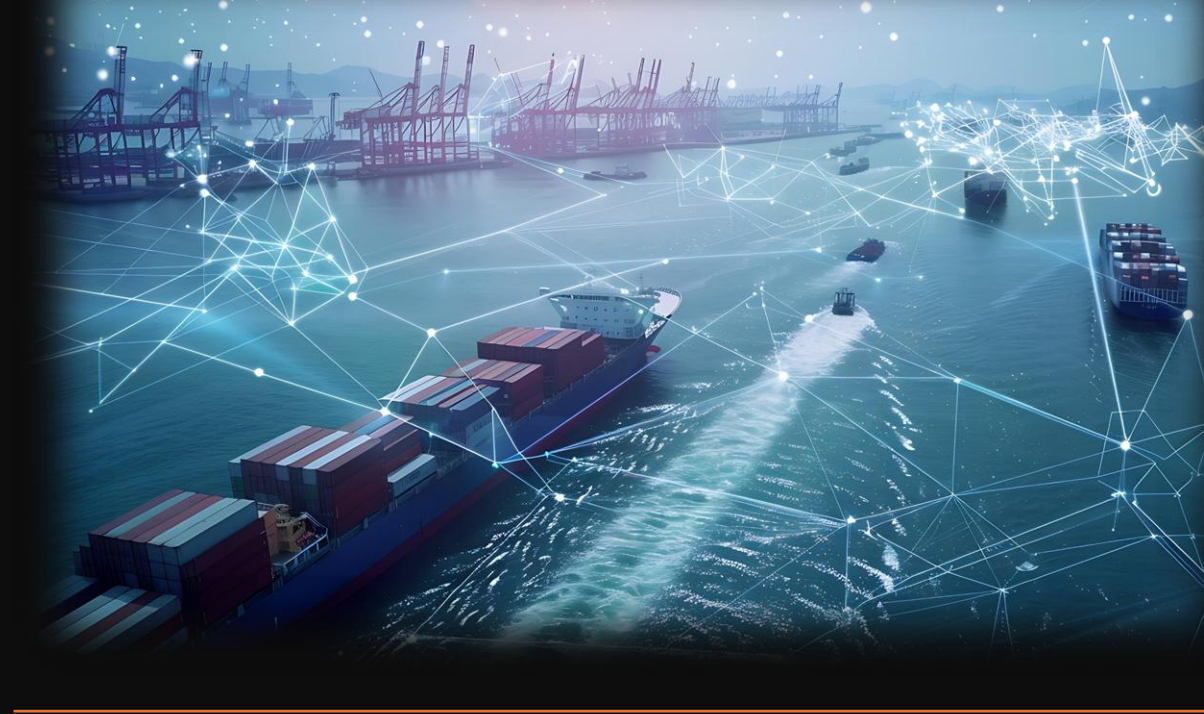
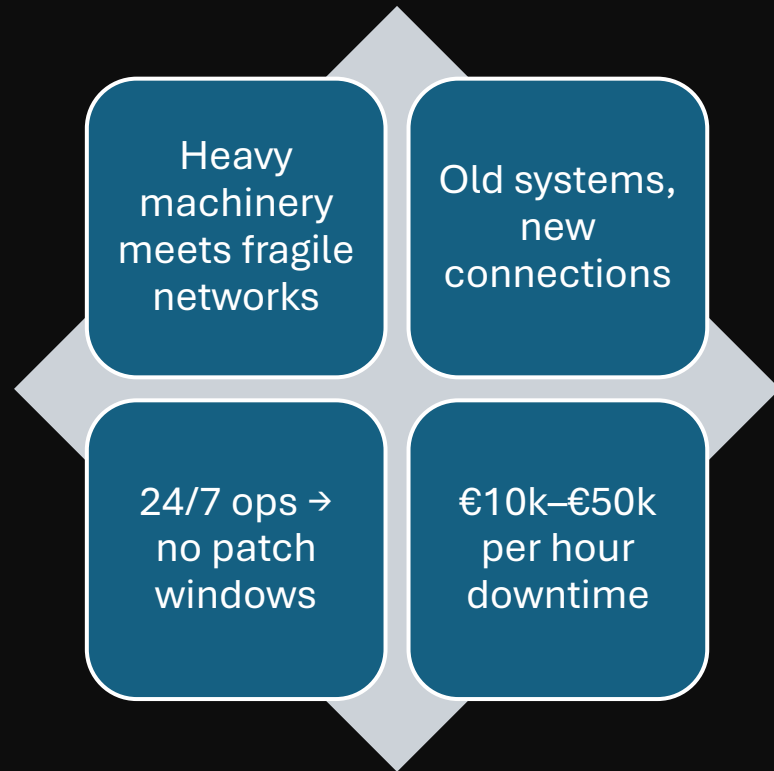
Threat Landscape 2025

- DP World Sydney – 4 ports offline → ~\$80M AUD loss
- AI reconnaissance tools mapping exposed industrial devices in minutes
- AI-generated phishing mimicking suppliers & operations
- “Cyber risk = lost tonnage”

“AI doesn’t change the threat - it speeds it up”



Why Bulk Terminals Are Unique



“Because every minute of uptime has a price tag.”

The terminal that thought it was offline

- No internet, no Wi-Fi — fully isolated.
- Updates done manually via USB.
- One firmware tool carried a hidden script.
- Result: entire loading system frozen for 48 hours.

“Air-gapped, and still hit.”



The login that opened the wrong door.

- Maintenance contractor logged in remotely.
- Reused credentials from another site.
- Credentials were part of a public breach list.
- Attackers logged in before anyone noticed.

“The login that opened the wrong door.”



The Multi-Vendor Mess

- Multiple vendors. No shared patching schedule.
- No single dashboard for network traffic.
- Faults misdiagnosed for days.
- Root cause: one unmonitored device.



“Five systems, zero visibility.”

Simple actions that keep cargo moving.

Action	Impact	Example Saving
Segment networks	Contain failures	Avoids 2-day outage
Harden gateways	Reduce exposure	Prevents €500k downtime
Control access	Stop credential reuse	Avoids 6-figure IR bill
5-page incident plan	Speedy recovery	40% faster response
Smart compliance	Satisfy insurers	Better premiums



The Future Threat Horizon

- AI reconnaissance tools
- Supply chain attacks
- Insurer scrutiny increasing
- OT/IT convergence → faster response

“Tomorrow’s threats move faster - so must recovery.”



Closing

- You can't defend what you can't see
- Downtime is the real enemy.
- Preparedness beats perfection.

Cybersecurity is no longer a technical issue - it's a business risk and a trust factor.

Your clients, your insurers, and your crews all depend on continuity.

The question isn't '***Are we secure?***' - it's '***How fast can we recover?***'

"Know your assets. Control your access. Test your defences. Stay operational."

