# Portfall: Maritime / Space Cyber Workshop – Scenario Summary for Facilitation Team

## Overview

**Scenario Name:** Portfall – Incident at Southgate Terminal  
**Duration:** 2 hours scenario + 1 hour debrief  
**Setting:** Southgate Maritime Terminal, a major Australian port  
**Type:** Cyber-physical simulation inspired by real-world port incidents (e.g. Maersk NotPetya, Houston Port attack)

This immersive simulation challenges teams to respond to a complex, unfolding cyberattack on port systems. The scenario blends realistic system disruptions, stakeholder pressure, legal ambiguity, and media escalation. Participants take on specific roles and must coordinate across functions to manage the incident in real-time.

## Workshop Teams & Roles

Each team will simulate an internal organisational unit. Participants are assigned to one of the following roles:

* **CEO / Executive:** Strategic decisions, external comms, approvals
* **Legal / Compliance:** Regulatory advice, breach reporting, insurer comms
* **Technical / Cyber:** Detect/respond to system anomalies, log analysis
* **Operations / Logistics:** Port throughput, scheduling, safety impacts
* **Media / Communications:** Public statements, social/media narrative control
* **Incident Coordinator / Scribe:** Logging, tagging, cross-role sync, debrief inputs

Each role has access to tailored injects, dashboards, policy documents, and VM systems to simulate real-world pressures.

## Facilitator Support Structure

In addition to the scenario participants, a dedicated Facilitation Support Team will guide the exercise in real-time.

Each facilitator will be assigned to support one of the six scenario roles:

|  |  |  |
| --- | --- | --- |
| **Scenario Role** | **Facilitator Assigned** | **Key Support Responsibilities** |
| Executive / CEO | [Insert Name] | Observe strategic decisions, nudge crisis declaration |
| Legal / Compliance | [Insert Name] | Track breach handling, prompt insurer comms |
| Technical / Cyber | [Insert Name] | Monitor log analysis, guide containment actions |
| Operations / Logistics | [Insert Name] | Support ops handoffs, watch for SOP use |
| Media / Communications | [Insert Name] | Track public messaging and internal morale handling |
| Incident Coordinator | [Insert Name] | Ensure logging fidelity and decision traceability |

**Facilitators will observe, nudge, and document — not lead.** They may prompt teams with timeline reminders, policy questions, or coordination nudges as needed to ensure realism and momentum.

All facilitators will convene every 30 minutes (eg., at T+30, T+60, or more often if required) for a brief internal sync to share cross-team insights and coordinate pressure pacing.

## Scenario Phases & Timeline

The exercise is divided into four escalating phases. Injects are delivered every 10–15 minutes. Each phase increases complexity and decision pressure.

**Phase 1: Disruption Emerges (T+0 to T+30)**

* Initial anomalies: AIS ship disappears, packet delays, expired contingency doc.
* CCTV flickers, media visibility spike begins.
* Teams must determine if escalation is required and begin formal logs.

**Phase 2: Public & Internal Chaos (T+30 to T+60)**

* Vendor email leak, GPS drift tweet, insurance contact begins.
* Scheduler shows corrupted data, manual ops may be needed.
* Roles face early coordination challenges and stakeholder confusion.

**Phase 3: Full Crisis Realised (T+60 to T+90)**

* Container misrouting, sabotage claims in media, morale breakdowns.
* Journalists arrive, insurer demands logs.
* Teams must align messaging, policy application, and containment actions.

**Phase 4: Resolution & Accountability (T+90 to T+120)**

* Final reports due: logs, breach notifications, media responses.
* CEO interview airs, government demands summary.
* Teams must close the incident with policy adherence and leadership clarity.

## Phase Details

### Facilitation Briefing: Running Portfall

**Portfall** is a 2-hour immersive cyber-physical simulation set at Southgate Maritime Terminal. This briefing is for the **facilitation team** responsible for guiding, observing, and supporting the participant teams throughout the scenario.

As a facilitator, your role is not to lead participants, but to **create realism, apply pressure, and support decision-making under stress**. Each facilitator is aligned to one of the core scenario roles, ensuring that participants receive realistic prompts, timeline nudges, and inject delivery at the right moments.

This is a live, role-driven exercise where the realism of the experience depends on discipline, timing, and adaptability. You are the invisible scaffolding behind the scenario.

### Facilitation Objectives

* Nudge teams when needed using prompts aligned to the scenario phase.
* Observe and document team decisions for post-scenario scoring and debrief.
* Maintain role consistency — speak and act only within your assigned domain.
* Flag any critical missteps, rule breaches, or exceptional decision points.

### Your Role

You are expected to:

* Know your assigned team’s expected decisions across all four phases.
* Be familiar with the associated dashboards, logs, and email injects.
* Use the provided facilitator scoring sheets and prompt questions during key decision windows.
* Coordinate with the lead facilitator or scenario controller every 30 minutes for pacing review.

**Your timing is essential.** This is not a presentation — it’s a dynamic, unfolding simulation. Teams will rise or falter based on their own decisions. Your job is to make the environment as real and high-stakes as possible.

### Phase 1: Disruption Emerges (T+0 to T+30)

* **Key Events:** AIS disruption (Ship\_Alpha disappears), CCTV flickers, emails note expired contingency docs.
* **Team Focus:** Early detection, ambiguity assessment. Tech should explore Node-04 anomalies. Legal should assess exposure from outdated documentation.
* **Media Role:** Spot early signals (MarineTracker spike). Begin prepping holding statement.
* **Executive Role:** Monitor developments, coordinate first status update.
* **Inject Types:** Emails, initial dashboard changes, internal warnings.

### Phase 2: Public & Internal Chaos (T+30 to T+60)

* **Key Events:** Vendor email chain leaks, tweet about GPS drift, AIS blackout.
* **Technical Team:** Detect and respond to scheduler anomalies, begin isolation if required.
* **Operations:** Consider switching to manual processes.
* **Legal:** Evaluate breach thresholds and prepare insurer response.
* **Media:** Coordinate messaging strategy. Respond to internal morale concerns.
* **Inject Complexity:** Overlapping triggers, increased role interdependence.

### Phase 3: Full Crisis Realised (T+60 to T+90)

* **Key Events:** Container misrouting confirmed, sabotage articles published, insurer formally requests logs.
* **Executive:** Must decide on media engagement strategy (CEO interview).
* **Legal:** Ensure logs are archived, begin breach draft.
* **Media:** Craft interview talking points, manage real-time narrative.
* **Ops:** Address crane control issues and communicate safety procedures.
* **Injects:** Tweets, log artefacts, insurer memos, morale emails.

### Phase 4: Resolution & Accountability (T+90 to T+120)

* **Key Events:** CEO media interview, breach notification sent, logs and reports due to government.
* **All Teams:** Finalise actions, close logs, export evidence.
* **CEO/Legal:** Deliver a unified external-facing summary. Respond to formal government inquiry.
* **Technical:** Submit forensics with timestamps and logs.
* **Media:** Issue final public statement (or choose to hold).
* **Coordinator:** Tag all artefacts for scoring, compile decision timeline.
* **Injects:** Ministerial report request, breach draft, tweet backlash, final log reminders.

## Success Criteria

Facilitators will evaluate teams on:

* Timeliness of responses
* Quality of decisions under pressure
* Cross-role coordination
* Policy application and logging

The final debrief will explore what worked, what failed, and how teams performed as a cohesive unit under pressure.

**Reminder:** This is a realism-focused workshop. Teams are expected to lead, not wait for prompts. Injects are designed to trigger real dilemmas. Let the scenario unfold organically and use logs, dashboards, and templates to guide your decisions.