Tabletop exercise kit for a port terminal

Three scenarios of 90 minutes each. Run one per session, or all three in a half day with breaks. Each scenario has a briefing, five injects with facilitator questions, and a hotwash (the debrief right after the discussion).

For: The people who run a terminal and the people who run its systems: terminal or operations manager, IT lead, OT and TOS administrator, gate supervisor, security officer, communications, and the manager who signs off.

Fictional scenarios. The scenarios are fictional. Times, systems and events are invented for discussion; they do not describe a real terminal or a real incident, and they contain no statistic.

Agenda of one scenario (90 minutes)

Start	Minutes	Step	What happens
0:00	10	Briefing	Objectives, ground rules, roles, the scenario's starting point.
0:10	65	Five injects	About 13 minutes per inject: read it, ask the questions, let the players decide.
1:15	15	Hotwash	What worked, what to improve, what to change in the plan; the note-taker reads back the actions.

Before the day

• Four weeks before: choose the scenario and the plan to test, set two or three objectives, name the facilitator and the note-taker.

• Two weeks before: adapt the injects to your systems (names of your TOS, gate and OCR systems; your shift pattern); invite the players in writing.

• One week before: send the participant cards; book a room with a table, a screen and a clock.

• On the day: name tents, participant cards on the table, players from different teams seated side by side.

Ground rules (read them at the briefing)

• No fault, no blame: the exercise tests the plan and the way people work together, not individuals.

• Answer with the plans, contacts and tools you have today, not the ones you wish you had.

• Decisions taken in the room set no precedent. Say what you would do, and who would decide.

• There are no trick questions and no hidden agenda.

• The scenario is artificial. If a detail does not fit your terminal, adapt it and keep going.

• What is said in the room stays in the room; only the after action report leaves it.

Roles

Role	Plays?	Does	Brings
Facilitator	staff	Runs the session: gives the briefing, reads each inject, asks the questions, keeps time and brings the discussion back to the objectives. Does not answer for the players.	This facilitator guide, the incident response plan being tested, a clock.
Note-taker (data collector)	staff	Records who decided what, when, with which information, and every gap between what the plan says and what people would do. Feeds the after action report.	The debrief template, a laptop or paper, the list of objectives.
Terminal or operations manager	player	Decides whether operations continue, slow down or stop; owns berth, yard and gate priorities.	The business continuity plan, the manual fallback procedures, the vessel schedule for the next 48 hours.
IT lead	player	Leads the technical response: scope, containment, evidence, restore.	The incident response plan, the network diagram, the backup and restore records, the support contracts.
OT and TOS administrator	player	Knows the terminal operating system, gate, OCR and crane interfaces, and the vendors' remote access.	The list of interfaces between the TOS and OT systems, the vendor contacts, the remote-access register.
Gate supervisor	player	Runs the truck gate: appointments, identity checks, release of cargo, queues.	The gate procedures, the manual processing form, the escalation contacts.
Security officer (FSO / CySO)	player	Links cyber and physical security, the Facility Security Plan and, where the rule applies, the Cybersecurity Plan. Knows who must be told, and by when.	The reporting criteria and contacts (authorities, police, port authority), the security plan.
Communications lead	player	Speaks to shipping lines, trucking companies, staff, the port community and the press, with one voice.	Prepared message templates, the customer and partner contact lists, the press contact rule.
Executive sponsor	player	Takes the decisions the plan reserves for management: shutdown, ransom, legal, insurer, public statements.	The delegation of authority, the contacts of the insurer and of legal counsel.
Observer	staff	Watches without playing: a partner, a vendor, a new manager. May ask a question through the facilitator.	Nothing but attention.

Scenario 1 · Ransomware on the terminal operating system

Night shift. The terminal operating system stops answering and a ransom note appears on several workstations. A vessel is due at the berth in the morning.

Objectives

• Test who detects, who decides to isolate, and how fast the decision reaches the right person.

• Test the manual fallback for gate, yard and vessel operations without the TOS.

• Test reporting to the authorities and communication to customers within the required time.

Players: Terminal or operations manager, IT lead, OT and TOS administrator, Gate supervisor, Security officer (FSO / CySO), Communications lead, Executive sponsor

0:00 · Briefing (10 min). Objectives, ground rules, roles, then read the starting point: Night shift. The terminal operating system stops answering and a ransom note appears on several workstations. A vessel is due at the berth in the morning.

0:10 · Inject 1 · 03:40, the screens stop

Yard planners report that the TOS screens freeze. Within minutes, three workstations in the control room show a message saying the files are encrypted and giving an address to contact. The gate is quiet; the night vessel operation is half done.

Facilitator questions

• Who is the first person called, by whom, and with which number?

• Who may decide to disconnect the TOS servers or the network, at 03:40, without waking the whole chain?

• Is the OT network (cranes, gate, OCR) separated from the office network? How do you know right now?

• What do you preserve before anyone restarts a machine?

What good looks like: A named on-call decision-maker, an isolation step written in the plan, evidence kept (screens photographed, machines not wiped).

0:23 · Inject 2 · 05:00, the scope grows

IT confirms that the TOS database server and the shared drives are encrypted. Nobody is sure yet whether the latest backup is clean. The night vessel operation has stopped. The gate opens at 06:00 and the first trucks are already queuing.

Facilitator questions

• Do you open the gate at 06:00? With which manual procedure, and which data (appointments, release list)?

• Where are the bay plans, the yard positions and the release status if the TOS is gone? On paper? Offline?

• Who decides to resume or suspend the vessel operation, and who tells the shipping line?

What good looks like: A manual fallback that has been tried before, offline copies of the data needed for the next shift, one person deciding.

0:36 · Inject 3 · 07:30, who must be told

Shipping lines and trucking companies start calling the customer desk. A port community group asks what is happening. A local journalist leaves a message.

Facilitator questions

• Is this a reportable incident? To whom, by when, and who signs the report? (US facilities: the National Response Center, 33 CFR 101.620 and 101.650. EU: NIS2 Article 23, early warning within 24 hours where it applies.)

• What do you say to customers in the first hour, when you do not know much yet?

• Who speaks to the press, and who approves the words?

What good looks like: Reporting criteria known in advance, a pre-approved holding message, one spokesperson.

0:49 · Inject 4 · 09:00, the demand

The attackers send a second message: they ask for a payment and say they have copied data, which they will publish if you do not pay.

Facilitator questions

• Who takes the decision on a ransom demand, and with whose advice (legal counsel, insurer, law enforcement)?

• Which data could have been copied: customer data, staff data, security plans?

• Who contacts law enforcement, and when?

What good looks like: The decision is reserved to a named executive in writing; the advisers' contacts are in the plan, not in someone's phone.

1:02 · Inject 5 · day 2, the restore

A clean backup is found. IT proposes to rebuild the servers and restore. Operations want the gate back on the TOS as soon as possible.

Facilitator questions

• In which order do you bring systems back, and who checks each one is clean before it rejoins the network?

• How do you reconcile what was done on paper (gate moves, yard moves) with the restored TOS?

• What do you change so that the same attack cannot happen again the same way?

What good looks like: A restore order agreed in advance, a reconciliation owner, a root-cause review with a date.

1:15 · Hotwash (15 min)

• What worked in the first hour?

• Which decision took longest, and why?

• Which part of the plan was missing, wrong or unknown to the people who need it?

• Which three actions do we take, who owns each, by when?

Scenario 2 · A fake truck with a spoofed appointment at the gate

A truck arrives with a valid appointment for an import container. The appointment was booked with a trucking company's real account, but that company never booked it.

Objectives

• Test the identity checks at the gate and the escalation when something does not match.

• Test the response to a compromised customer account on the appointment or community system.

• Test evidence preservation and coordination with the cargo owner, the shipping line and the police.

Players: Terminal or operations manager, IT lead, OT and TOS administrator, Gate supervisor, Security officer (FSO / CySO), Communications lead

0:00 · Briefing (10 min). Objectives, ground rules, roles, then read the starting point: A truck arrives with a valid appointment for an import container. The appointment was booked with a trucking company's real account, but that company never booked it.

0:10 · Inject 1 · 14:10, at the in-gate

A truck presents an appointment and a release reference for an import container. The appointment is valid in the system. The clerk notices that the driver is not on the list of drivers the trucking company usually sends, and the truck's plate is not known either.

Facilitator questions

• What do your clerks check before a container leaves: appointment, release, driver identity, plate, company?

• What may a clerk do on their own when something does not match? Hold the truck? Call whom?

• How long can a truck be held, and who decides?

What good looks like: Written checks at the gate, a clear hold-and-escalate rule, a named person reachable in minutes.

0:23 · Inject 2 · 14:25, the real company calls back

The trucking company says it did not book this appointment. Its account on the appointment system was used from a connection it does not recognise. The truck leaves the queue before anyone stops it.

Facilitator questions

• Who suspends the account, and how do you check every other appointment it booked?

• Which logs do you keep, and who asks for the gate camera recordings before they are overwritten?

• Who tells the cargo owner and the shipping line?

What good looks like: Account suspension in minutes, logs and camera footage preserved, the cargo owner told the same day.

0:36 · Inject 3 · 16:00, it happened before

Reviewing the account's history, IT finds two other containers released earlier in the week through appointments booked from the same connection.

Facilitator questions

• Who reports this, to whom (police, customs, the port authority, the security authority), and when?

• Is this a reportable cyber incident under the rules that apply to you? Who decides?

• What do you tell the other trucking companies today?

What good looks like: Reporting criteria for cargo crime and for cyber incidents known in advance; one owner for the case.

0:49 · Inject 4 · day 2, how it started

The trucking company finds that one of its dispatchers answered an email that looked like it came from the terminal, asking to reset the password on the appointment system.

Facilitator questions

• Does your appointment system require multi-factor authentication for customer accounts? Could it?

• How do customers know an email really comes from you?

• Who helps the trucking company, and where does your responsibility stop?

What good looks like: A decision on multi-factor authentication, a known channel for genuine messages, a warning sent to the community.

1:02 · Inject 5 · day 3, the next shift

Operations ask what changes at the gate from tomorrow morning, without creating a queue.

Facilitator questions

• Which check do you add for release (driver identity, a one-time release code, a callback)?

• How do you train the clerks on it, and who checks it is applied?

• How will you know if the same method is tried again?

What good looks like: One practical change at the gate, a briefing for every shift, an alert on unusual booking patterns.

1:15 · Hotwash (15 min)

• Did the clerk know they were allowed to stop the truck?

• How long did it take to suspend the account and preserve evidence?

• Who owned the case end to end?

• Which three actions do we take, who owns each, by when?

Scenario 3 · An OCR and gate camera outage at peak time

Morning peak. The gate OCR stops reading container numbers and plates. Lanes slow down and the queue grows towards the public road. Nobody knows yet whether it is a fault or an attack.

Objectives

• Test the manual gate procedure and the decision to switch to it.

• Test how the team tells a technical fault from a cyber incident, and the control of vendor remote access.

• Test communication with truckers and local authorities, and the reconciliation of data afterwards.

Players: Terminal or operations manager, IT lead, OT and TOS administrator, Gate supervisor, Security officer (FSO / CySO), Communications lead

0:00 · Briefing (10 min). Objectives, ground rules, roles, then read the starting point: Morning peak. The gate OCR stops reading container numbers and plates. Lanes slow down and the queue grows towards the public road. Nobody knows yet whether it is a fault or an attack.

0:10 · Inject 1 · 07:05, the lanes slow down

The OCR portal stops returning container numbers and plates. Clerks have to type every transaction. The time per truck rises and the queue reaches the terminal entrance.

Facilitator questions

• Who decides to switch to the manual gate procedure, and is it written down?

• Do you have enough clerks and forms for manual processing at peak time?

• What about damage inspection photos that the OCR portal normally takes?

What good looks like: A written manual procedure with a trigger, staff who have practised it, a way to record damage without the cameras.

0:23 · Inject 2 · 07:30, fault or attack?

The OT administrator sees that the camera server rebooted twice during the night and that its configuration changed. The vendor's support line says it is investigating and asks to connect remotely.

Facilitator questions

• How do you tell a fault from an attack? Who looks at what, first?

• Do you let the vendor connect now? Through which access, approved by whom, logged where?

• Was the configuration change planned? Where would you see it?

What good looks like: A change log to compare with, a remote-access procedure that is used even under pressure, logs kept before any fix.

0:36 · Inject 3 · 08:15, the queue reaches the road

The truck queue reaches the public road. The local police call the gate. Trucking companies are posting about the waiting time.

Facilitator questions

• Who talks to the police and the local authority, and what traffic plan do you have?

• Do you reschedule appointments or ask trucks to come back later? Who tells them, how?

• Do you prioritise some cargo (reefers, dangerous goods, vessel cut-off)?

What good looks like: A congestion plan agreed with the local authority, a message to the trucking community, clear priorities.

0:49 · Inject 4 · 10:00, errors appear

Customer service reports containers recorded with wrong numbers during manual entry, and a container gated out against the wrong appointment.

Facilitator questions

• How do you find and correct the errors made during the outage?

• Who checks the release status of every container that left during manual processing?

• What do you tell the customers concerned?

What good looks like: A reconciliation owner, a list of every transaction done by hand, a check of each release.

1:02 · Inject 5 · 13:00, back online

The OCR works again after the vendor restored the previous configuration. The vendor cannot yet explain the change.

Facilitator questions

• What evidence do you ask the vendor for, and by when?

• Is this a reportable incident? Who decides, with which information?

• What do you change in the contract or the remote-access rules?

What good looks like: A written root-cause report requested from the vendor, a decision on reporting, a change to remote access if needed.

1:15 · Hotwash (15 min)

• How long did it take to switch to manual, and who decided?

• Did anyone ask whether it was an attack before the vendor connected?

• What did the outage cost in data quality, and how do we prevent it next time?

• Which three actions do we take, who owns each, by when?

After action report (debrief template)

Fill this in during the hotwash and within a week of the exercise. It is the after action report: keep it with your exercise records, and use it to update the plan.

Section	What to write	Notes
Exercise	Name, date, place, duration, scenario number.	
Purpose and objectives	The plan tested and the two or three objectives set beforehand.	
Participants	Roles present (not names, if the report will travel), facilitator, note-taker, observers.	
What worked	Decisions taken quickly, procedures that were known and used.	
What to improve	Delays, missing contacts, unclear authority, procedures nobody knew.	
Plan gaps	What the plan says that people would not do, and what people would do that the plan does not say.	
Actions	One line each: action, owner, due date, status. Review them at the next exercise.	
Compliance record	Where this report is filed, for the drills and exercises your rules require.	

Actions

#	Action	Owner	Due date	Status
1				
2				
3				
4				
5				
6				

Hotwash order

- Each player: one thing that worked, one thing to improve (2 minutes each).
- The facilitator: the objectives, met or not.
- The note-taker: reads back the decisions and the gaps recorded.
- Together: three actions, each with an owner and a date.

Why exercise (public sources)

A tabletop is a discussion, not a test of equipment

NIST describes tabletop exercises as discussion-based events where a facilitator presents a scenario and asks questions, to validate the content of plans such as incident response plans; they typically last two to eight hours (SP 800-84, section 4). *(NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (section 4 and appendix A: tabletop exercises, facilitator and participant guides, after action report), September 2006)*

Public scenarios exist for ports

CISA publishes free Tabletop Exercise Packages, including a Maritime Ports situation manual, with a 20-minute briefing, two 60-minute modules and a 20-minute hotwash. *(CISA, Maritime Ports CTEP Situation Manual (cybersecurity scenarios), November 2023)*

The IMO guidelines ask for practice

The functional elements Respond and Detect ask organisations to develop, implement and practise their activities, and knowledge should be tested, for example through drills and exercises (paragraph 3.5). *(IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (paragraph 3.5: Detect, Respond, Recover; drills and exercises), 28 May 2026)*

ENISA asks ports for annual exercises

Good practice PS-18: annual training exercises that involve the critical port stakeholders, with formal post-exercise reports; OP-15: test incident procedures through exercises. *(ENISA, Port Cybersecurity: Good practices for cybersecurity in the maritime sector (PS-18 annual exercises and post-exercise reports, OP-15), November 2019)*

In the US, exercises are in the rule

Under its Cybersecurity Plan, an MTSA facility runs at least two cybersecurity drills and one exercise each calendar year, no more than 18 months apart; the exercise can be a tabletop (33 CFR 101.635). *(eCFR, 33 CFR 101.635, Drills and exercises (US Coast Guard cyber rule, subpart F), in force since 16 July 2025, checked 11 November 2026)*

Sources (public, dated)

NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (section 4 and appendix A: tabletop exercises, facilitator and participant guides, after action report), September 2006. https://csrc.nist.gov/pubs/sp/800/84/final

CISA, CISA Tabletop Exercise Packages (CTEP): templates, scenarios, discussion questions, after action report, service page, checked 11 November 2026. https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISA, Maritime Ports CTEP Situation Manual (cybersecurity scenarios), November 2023. https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios

ENISA, Port Cybersecurity: Good practices for cybersecurity in the maritime sector (PS-18 annual exercises and post-exercise reports, OP-15), November 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

ENISA, Guidelines: Cyber Risk Management for Ports (PS-18 maturity: drills, exercises and lessons learned), December 2020. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (paragraph 3.5: Detect, Respond, Recover; drills and exercises), 28 May 2026. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

eCFR, 33 CFR 101.635, Drills and exercises (US Coast Guard cyber rule, subpart F), in force since 16 July 2025, checked 11 November 2026. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F

Directive (EU) 2022/2555 (NIS2), Article 23: reporting obligations, 14 December 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this kit, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/training/tabletop-exercise-kit/ . The scenarios are fictional. Times, systems and events are invented for discussion; they do not describe a real terminal or a real incident, and they contain no statistic. This kit is a discussion tool written by Port Cyber Alliance from public guidance. It does not replace your incident response plan, your regulator's instructions or your legal counsel. Port Cyber Alliance does not certify or audit terminals.