Tabletop exercise kit for a port terminal: participant cards

One card per role: print it, cut it, put it on the table with the name tent. Then one handout per scenario, without the facilitator's questions.

Ground rules

• 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.

Role cards (cut along the lines)

Terminal or operations manager

Your part: Decides whether operations continue, slow down or stop; owns berth, yard and gate priorities.

Bring: The business continuity plan, the manual fallback procedures, the vessel schedule for the next 48 hours.

Think about: Which operations can run without the TOS, and for how long? Who must agree before you stop the gate or a vessel operation?

Name: _____

IT lead

Your part: Leads the technical response: scope, containment, evidence, restore.

Bring: The incident response plan, the network diagram, the backup and restore records, the support contracts.

Think about: What can you isolate without stopping operations? Where are the backups, and when was a restore last tested?

Name: _____

OT and TOS administrator

Your part: Knows the terminal operating system, gate, OCR and crane interfaces, and the vendors' remote access.

Bring: The list of interfaces between the TOS and OT systems, the vendor contacts, the remote-access register.

Think about: Which vendor can connect to what, today, and who can switch that access off?

Name: _____

Gate supervisor

Your part: Runs the truck gate: appointments, identity checks, release of cargo, queues.

Bring: The gate procedures, the manual processing form, the escalation contacts.

Think about: What do your clerks check before a container leaves, and what do they do when something does not match?

Name: _____

Security officer (FSO / CySO)

Your part: 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.

Bring: The reporting criteria and contacts (authorities, police, port authority), the security plan.

Think about: Which events in this scenario are reportable, to whom, and who signs the report?

Name: _____

Communications lead

Your part: Speaks to shipping lines, trucking companies, staff, the port community and the press, with one voice.

Bring: Prepared message templates, the customer and partner contact lists, the press contact rule.

Think about: What do you say in the first hour, when you do not know much yet? Who approves it?

Name: _____

Executive sponsor

Your part: Takes the decisions the plan reserves for management: shutdown, ransom, legal, insurer, public statements.

Bring: The delegation of authority, the contacts of the insurer and of legal counsel.

Think about: Which decisions only you can take, and what do you need on the table to take them?

Name: _____

Scenario 1 handout · 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.

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.

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.

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.

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.

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.

Your notes

Scenario 2 handout · 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.

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.

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.

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.

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.

Inject 5 · day 3, the next shift

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

Your notes

Scenario 3 handout · 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.

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.

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.

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.

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.

Inject 5 · 13:00, back online

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

Your notes

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.