Incident Decision Tabletop

Secondary, higher ed, professional | Runbook | 60-120 minutes

Before class: This is an instructor preparation runbook. Assemble the fictional scenarios, messages, or data it specifies before use; it does not provision a lab or include a ready-made dataset.

Lab ID: TABLETOP-IR-01 Outcome: Coordinate technical, operational, privacy, legal, and communication decisions during a fictional incident. Environment: Scenario packet and role cards. Time: 60-120 minutes.

Roles

- Incident coordinator
- Security analyst
- IT or service owner
- Privacy or records lead
- Legal or compliance advisor
- Communications lead
- Executive sponsor
- User or community representative

Scenario Design

The starting packet should include:

- Mission and critical services
- Known and unknown facts
- Initial technical indicators
- Affected users or data categories
- Recovery dependencies
- Contact and authority structure

Injects may include new evidence, a service outage, media inquiry, unavailable backup, third-party notification, or accessibility concern.

Decision Log

Time: _____

New information: _____

Decision: _____

Reason: _____

Dissent or unresolved issue: _____

Owner: _____

Next review: _____

Evaluation

Assess prioritization, evidence, coordination, communication, protection of people and mission, recovery thinking, and documentation. Do not score one predetermined response as the only acceptable answer when multiple defensible options exist.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Runbook 5 - Incident Decision Tabletop.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/incident-decision-tabletop/