Module 5
Incident Coordination Lab

Student Guide

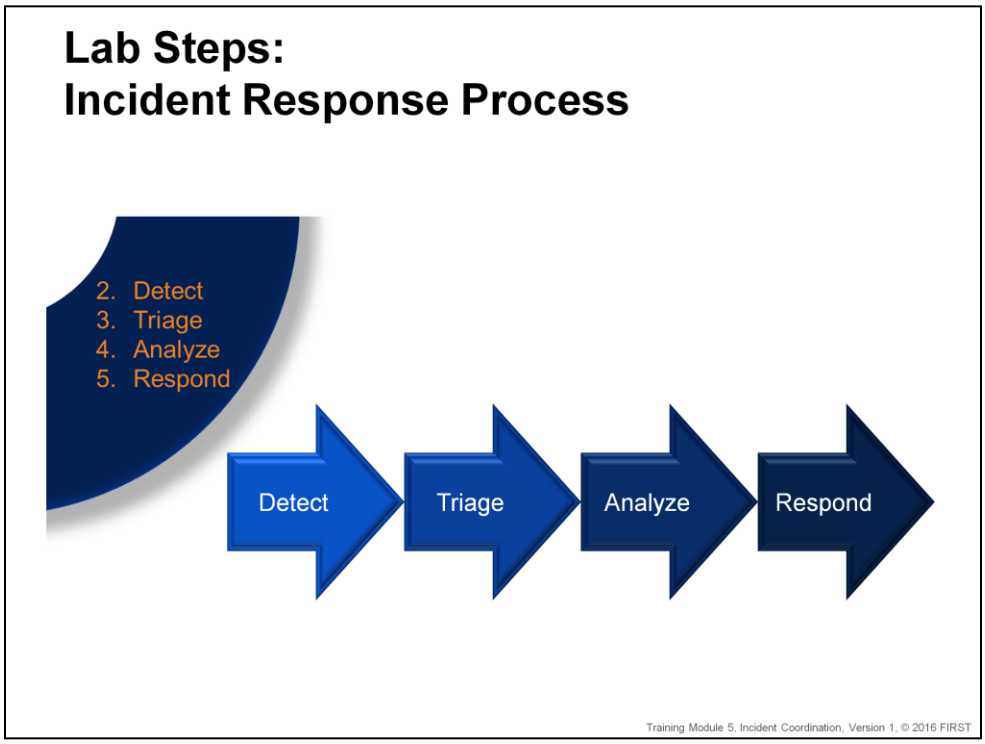
Lab Introduction

- Open your Lab Student Guide
- Your instructor will guide you through each step

Training Module 5, Incident Coordination, Version 1, © 2016 FIRST

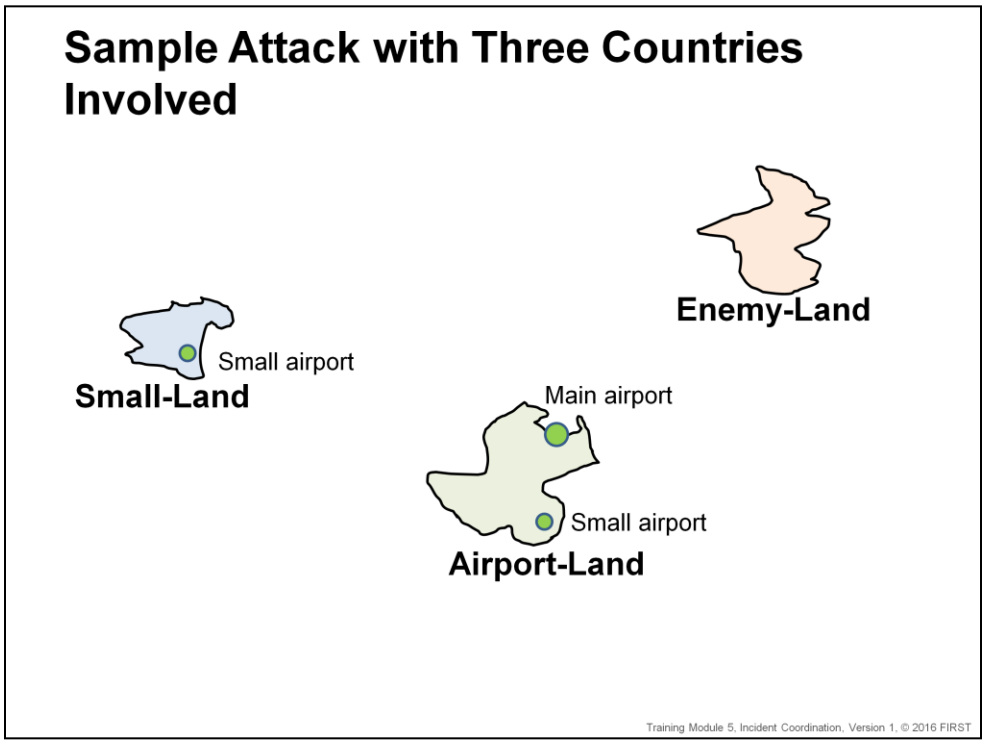
Lab Introduction

We will use the Incident Coordination steps to walk through four related scenarios, as a guided exercise that your instructor will lead. We will stop to ask and answer questions along the way.



Lab Steps: Incident Response Process

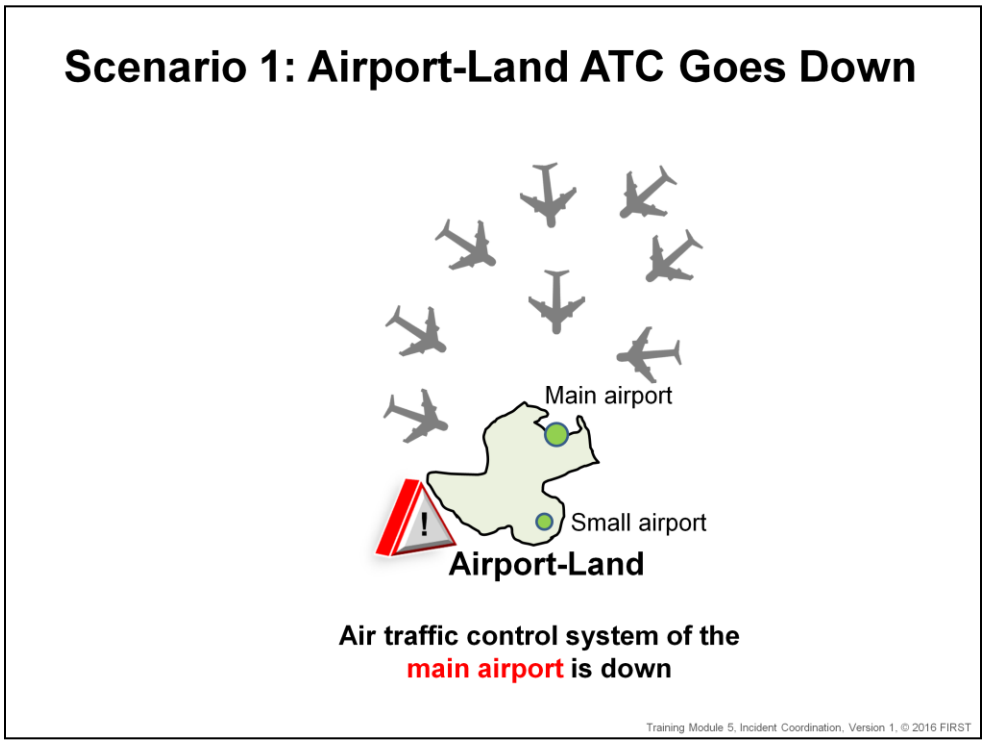
You will use the Incident Response steps outlined in the course to develop an action plan for addressing this incident. Keep these steps in mind as we proceed through the lab.



Sample Attack with Three Countries Involved

There are three countries involved in this scenario.

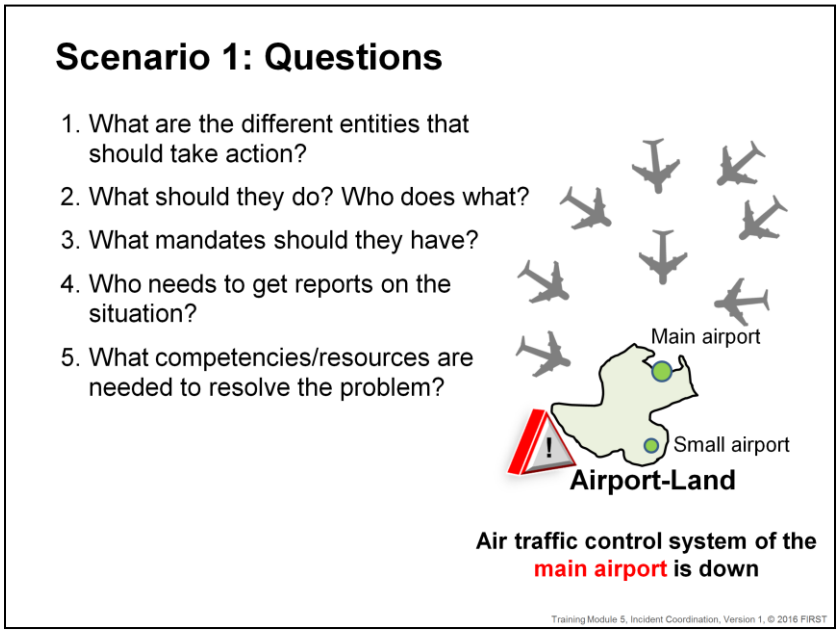
- Airport-Land has the main airport of the region. It also has a second, smaller airport. Airport-land has a good relationship with Small-Land and a neutral relationship with Enemy-Land.
- Small-Land is a “friendly” country. It depends on Airport-Land’s main airport.
- Enemy-Land is not a friendly country and is at times considered an enemy.



Scenario 1: Airport-Land ATC Goes Down

The air traffic control, or ATC, system of the main airport in Airport-Land is completely down.

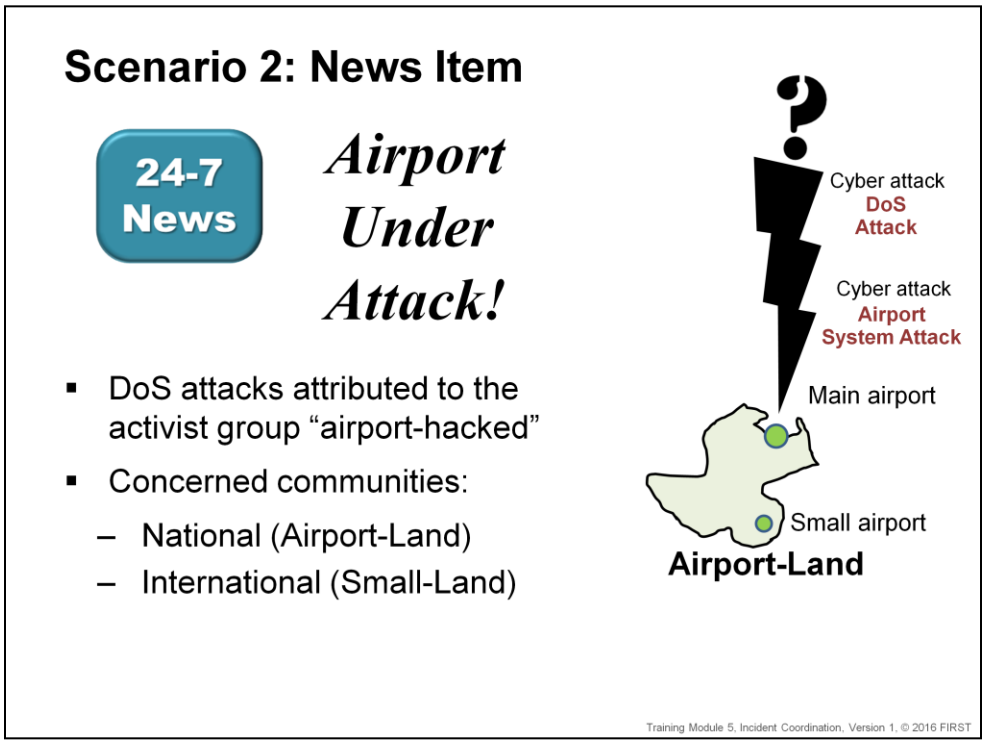
- Air-traffic congestion is critical.
- The airport technology director reports suspicious activity in the ATC.
- The regional ATC escalation team is not in your city and they are not answering calls.
- The available IT team is not very knowledgeable about the ATC application.



Scenario 1: Questions

Now let's walk through some questions.

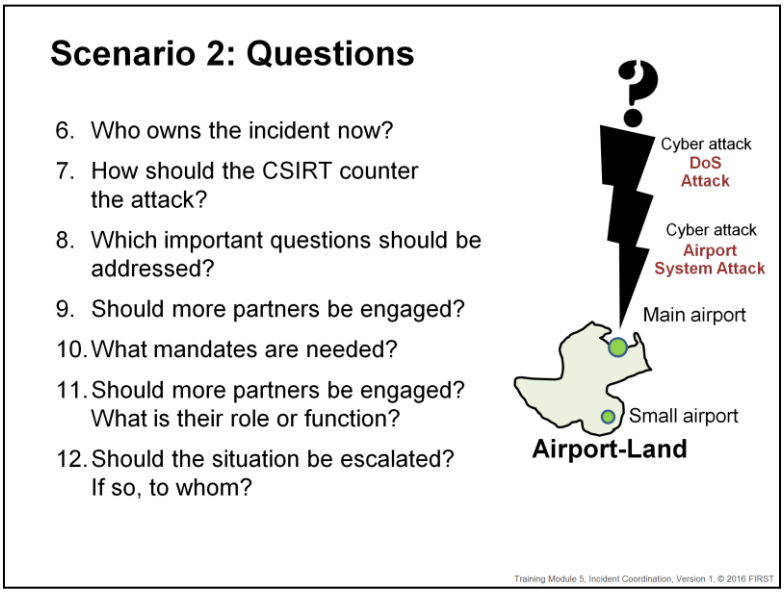
1. What are the different entities that should take action?
2. What should they do? Who does what?
3. What mandates should they have?
4. Who needs to get reports on the situation?
5. What competencies and resources are needed to resolve the problem?



Scenario 2: News Item

Let’s look at another scenario, starting with a news item: “Airport Under Attack!”

- During analysis, a series of denial of service, or DoS, attacks are detected. They are attributed to an activist group called “airport-hacked.”
- The news media has heard about the attack and is putting out headlines such as “Alert. Airport down. Attack….”
- There is concern within the national and international communities about DoS attacks plus anything else imaginable such as worms, Web portal attacks, and other kinds of attacks.



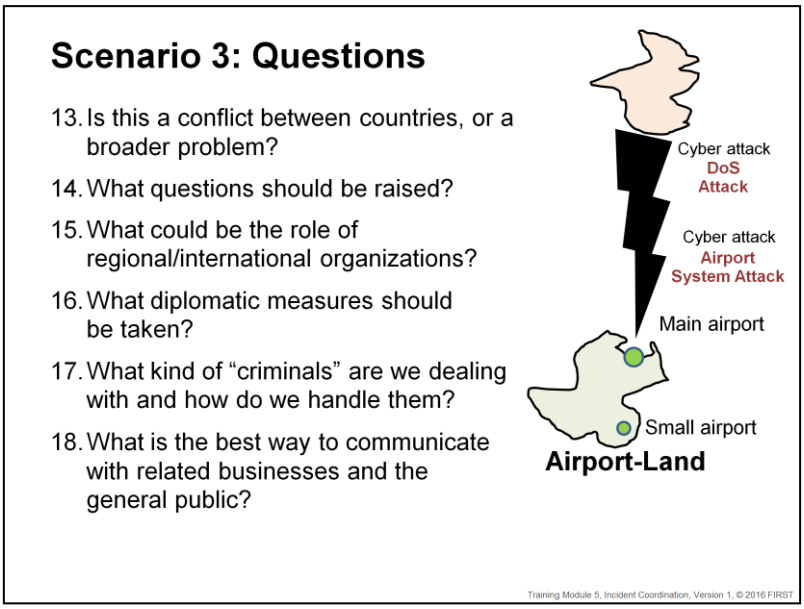
Scenario 2: Questions

Now let's walk through some more questions.

6. Who owns the incident now?
7. How should the CSIRT counter the attack?
8. Which important questions should be addressed?
9. Should more partners be engaged? What is their role or function?
10. What mandates are needed?
11. Should more partners be engaged? What is their role or function?
12. Should the situation be escalated? If so, to whom?

Scenario 3: News Item

Now let's look at another scenario, starting with another news item: The attack is attributed to a neighboring country.



Scenario 3: Questions

Now let's walk through some more questions.

13. Is this a conflict between countries, or a broader problem?

14. What questions should be raised? How can the CSIRT community and the FIRST organization help?

15. What could be the role of regional and international organizations?

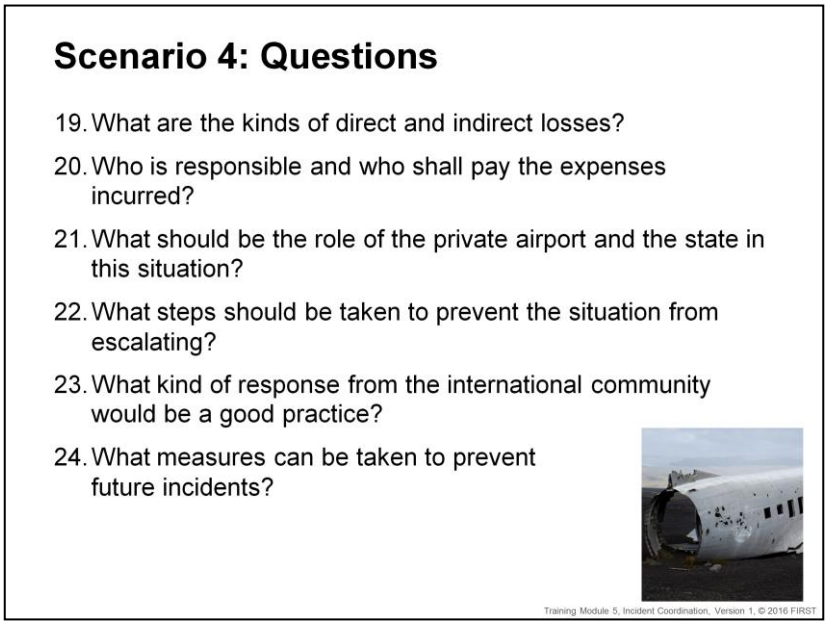
16. What diplomatic measures should be taken?

17. What kind of "criminals" are we dealing with and how do we handle them?

18. What is the best way to communicate with related businesses and the general public?

Scenario 4: News Item

Now let's look at yet another scenario, starting with another dire news item: Due to the ATC outage, a plane crashes, killing all on board.



Scenario 4: Questions

Now let's walk through some more questions.

19. What are the kinds of direct and indirect losses?

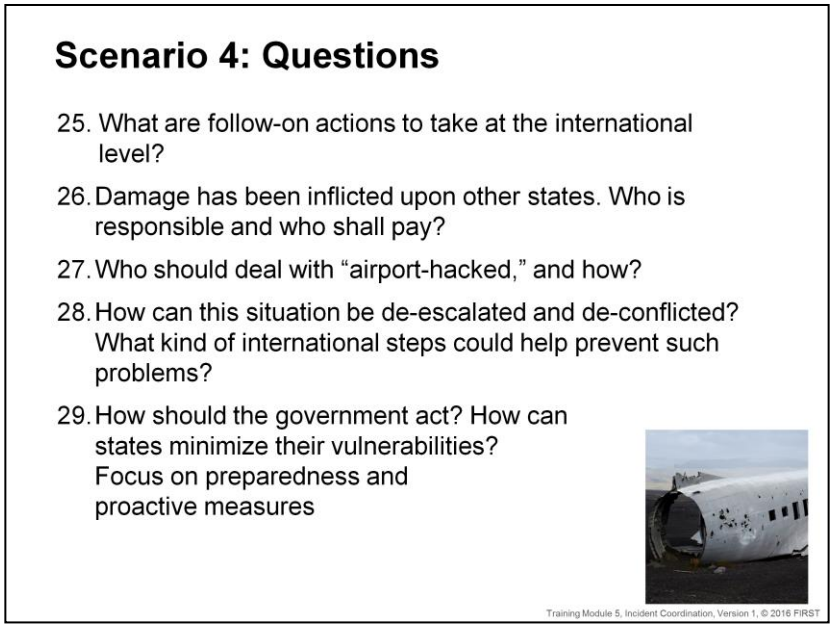
20. Who is responsible and who shall pay the expenses incurred?

21. What should be the role of the private airport and the state in this situation?

22. What steps should be taken to prevent the situation from escalating?

23. What kind of response from the international community would be a good practice?

24. What measures can be taken to prevent future incidents?



Scenario 4: Questions (continued)

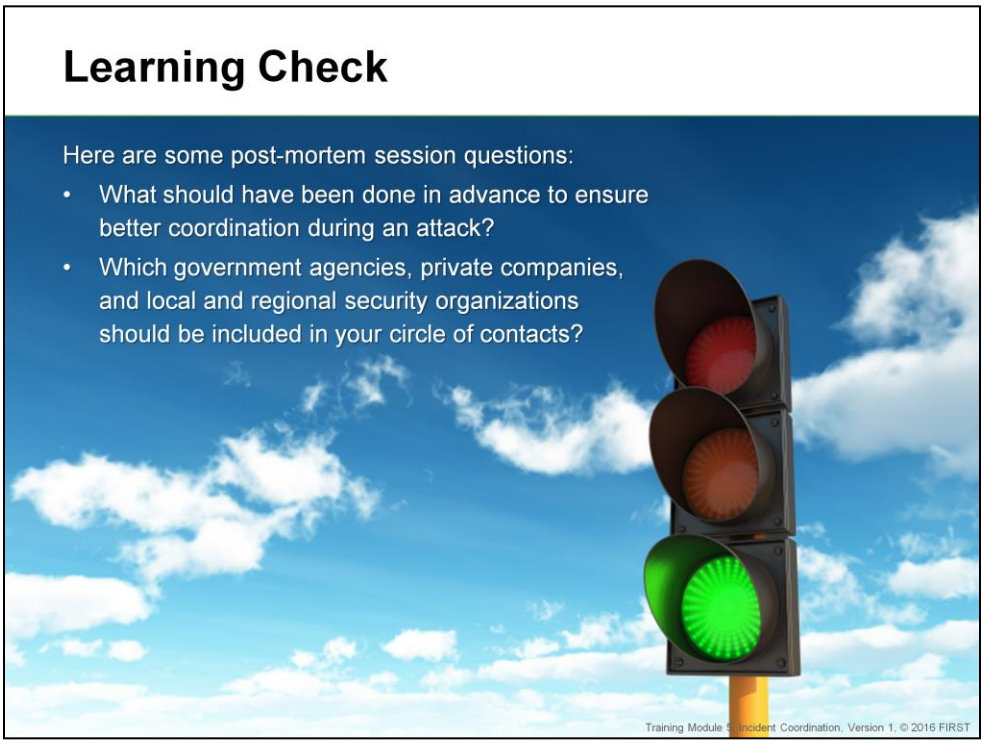
25. What are follow-on actions to take at the international level?

26. Damage has been inflicted upon other states. Who is responsible and who shall pay?

27. Who should deal with “airport-hacked,” and how?

28. How can this situation be de-escalated and de-conflicted? What kind of international steps could help prevent such problems?

29. How should the government act? How can states minimize their vulnerabilities? Focus on preparedness and proactive measures.



Learning Check

Here are some post-mortem session questions:

- What should have been done in advance to ensure better coordination during an attack?
- Which government agencies, private companies, and local and regional security organizations should be included in your circle of contacts?