SAND2013-0076P

Guided Exercise

PHBC Physical Security and MC&A

Goal: This exercise will be used to give students some practice identifying ways to minimize risk associated with a biosecurity threat. Students will work through a set of questions about physical security and MC&A to think about physical security design for a laboratory. This exercise is intended for students who have a basic understanding of the principals of laboratory biosecurity. It builds upon basic knowledge of biosecurity risk assessment.

Know:

- That a risk assessment supports appropriate physical security mitigation strategies
- Options for securing a laboratory
- That a robust MC&A system is part of an overall physical security plan

Feel

- Confident that proposed physical security measures will protect the asset

Do

- Create a mock physical security system for a laboratory
- Think about ways MC&A can be used to secure assets

Materials:

- Instructor notes
- Scratch paper for students to take notes
- Extra pens for notes
- Big dry erase board or flip chart
- Table and chairs to work on worksheet
- Laboratory for observation
- References for instructors – GBRMC Physical Security Course, Access and Accountability Course
- Students should bring their notes on the Biosecurity section of the course.
- Translated worksheet
- Interpreter for discussion

Instructor Notes:

This exercise will primarily be inquiry driven, meaning that the students will be given some time to work on the exercise and the instructor will be there to help them work through the questions (not just give them the answers).

The students will be given a mock scenario, which they will use to suggest physical security mitigation controls. It is expected that not all of the students will be very familiar with the different mitigation options, so the instructors are encouraged to explain them as they work through the exercise.

A key point to demonstrate is how a risk assessment can support appropriate physical security mitigation strategies. The students should be prepared to defend their mitigation strategy – and their answer should always be because either the risk assessment warrants it or it doesn't. The overall goal is to have an in depth conversation about physical security and the theory and options for securing a laboratory. How in depth this conversation gets will depend on the background and student interest.

Time	**Step: Description of Activity**	**Notes**
5 min	1. Introductions. Review Goals, Objectives, timeframe 2. Pass out worksheet.	Verbally review the goals of the exercise as well as the objectives listed above - read
5 min	3. Brief PHBC Laboratory Tour - pointing out features of physical security and MC&A. For example, identifying access controls, identification procedures, locked freezers, cameras, etc., 4. Instructors should talk through the questions on the handout, answering them with regard to PHBC, using it as an example.	It should be noted that PHBC may not have much in terms of physical security measures. So the instructors should ask the students why that is. Expected response: a risk assessment was done and it was not deemed necessary. Factors that contribute to the assessment are: the agents and agent properties, cost, stability of the region, current infrastructure and practices and procedures, potential threats. The main idea here is to get the students to associate and consider a risk assessment before suggesting physical security or MC&A mitigation measures. Instructors should be warned not to give out any specific information about PHBC because security plans are by nature sensitive. If necessary a conversation about sharing information and securing security plans could take place.
10 min	5. Next the students will be led to an	The instructors who will help guide

	area where they can work through a hypothetical scenario to think about designing a physical security system for a laboratory. 6. Allow the students to read the scenario and work through the worksheet questions. 7. Scenario: Pretend that this is your lab and that you are researching the prevalence of pandemic influenza virulence factors present in patient specimens. Routine procedures in the laboratory include: cell culture, ELISA, PCR and bioinformatics. Recently, the region has become very unstable, in terms of resources, money, electricity, and possible threats in the region. How do you secure the laboratory? 8. Student instructions: In your group spend 10 minutes to identify ways to better secure the assets of this laboratory using physical security mitigation measures. The questions below will help you with this task. Please discuss how you would detect, delay and respond to potential intruders and how you would control access. Be prepared to report out to the instructor. 9. Students will work through questions on the worksheet.	the students through the scenario and help the students work through the questions. Do your best to keep them on track so that they don't spend the whole time on the first question. The main goal here is to have a focused conversation about physical security. Expected responses for the worksheet are below. Allow students to draw a laboratory schematic picture if it helps them to visualize the physical security measures.
5 min	10. Plenary Discussion – discuss the pros and cons of each physical security design component that the students came up with.	After the students have been given 10 minutes to work through the worksheet, have the students present their physical security plan. The instructor can then lead a plenary discussion to re-cap the correct responses and the importance of each physical security aspect.

5 min	11. Review Plenary Discussion – Ask the students what they learned, what it means, and where to go from here?	Instructors will ask for any additional questions and answer them. If additional questions exist – they can be put in the parking lot and addressed at a later time.
30 min total	Evaluation - Dismiss	Pass out Level 1 evaluations KFD for the students. After activity Instructors will fill out Level 2 evaluations.

Designing a Physical Security System

Scenario:

Pretend that this is your lab and that you are researching the prevalence of pandemic influenza virulence factors present in patient specimens. Routine procedures in the laboratory include: cell culture, ELISA, PCR and bioinformatics. Recently, the region has become very unstable, in terms of resources, money, electricity, and possible threats in the region. How do you plan to secure the laboratory?

In your group spend 10 minutes to identify ways to better secure the assets of this laboratory using physical security mitigation measures. The questions below will help you with this task. Please discuss how you would detect, delay and respond to potential intruders and how you would control access. Be prepared to report out to the instructor.

1. Identification of the assets
    a. Where in the laboratory space will the agents be stored and used in your protocol? How will the assets be accounted for? In the BSL2 Laboratory in the freezer. Labeling system, accountable people, inventory logs and periodic checks, performance reviews. This is where a conversation about appropriate MC&A Practices can be included.

    b. Are there other assets such as equipment used in the protocol that may require physical protection? Explain. Centrifuges, PCR machines, ELISA readers are all very valuable and may have a dual use so they should be secured, however, the computers containing data about the virulence factors including sequence data, with bioinformatics results, would be potentially the most important in this case to keep secure. Ways to keep it secure is to password protect the computer, files, not leave the desktop open. Have a backup copy of data that is on a secure server.

2. Design System

a. Define any special *exclusion, exclusion and limited areas.* Students can write the boundaries for these areas on a simple diagram that they create. The special exclusion areas should be areas where only very specialized staff are allowed – this could be the tissue culture room where live virus is cultured and also the freezer (only certain personnel can get access to the stock freezer – secured with a lock). The exclusion area will be the laboratory itself – likely there are other projects happening in the laboratory that are not as sensitive as the influenza project. For example, routine diagnostics. This area is still exclusion because only trained laboratory staff are allowed in this area – the general public, administrators, and others are restricted from this area unless accompanied by an escort (who can keep an eye on the person, minimizing the risk of the person getting exposed to the virus as well as inhibiting the person from stealing the virus). The limited area is the building itself, which may have offices for a variety of people, many of which may not work in the actual laboratory. The limited area is restricted to those who do not have a need to enter the building, and there should be a procedure to follow for those who do need to be in the building.

Instructors ask the students why they marked the boundaries where they did – make sure it is a risk-based reason/answer.

Note: the points of entry for both areas should be labeled on the diagram. Entry is generally, through the doors – but instructors should also ask about the windows and make sure that they are secured as well. Ask the students about what type of access controls could be used to further define the boundaries between the areas.

The main idea here is that there should be stronger access controls for the special exclusion and exclusion areas than the limited areas, but the limited areas should still have something. The students may not be familiar with some of the options for access controls – provide them examples. Examples include a specialized key granting system, electronic swipe cards, hand readers – something someone has, something someone knows, something someone is. The point here is that it doesn't necessarily have to be fancy, but it does need to protect the asset with a robust system. A conversation about electricity stability here may be useful – stating that you may want a system that has a back up power supply. Instructors make sure it is a risk-based reason/answer.

b. Describe features that will help detect an intruder, delay an intruder and respond to the intruder in your physical security system. Sensors should be appropriate to the type of traffic that would trigger them, for example: balanced magnetic switches on doors/windows or microwave or passive infrared sensors. To facilitate delay the sensors should be placed in an area that will allow

detection, assessment and response to happen in a time frame that the adversary can be apprehended – delay (Locked doors, perimeter fencing, solid doors, vehicle barriers, bars on windows, magnetic locks on doors, locks on freezers and cabinets, guards), if possible. Talk about the role of the guards of the facility – who do they call if a sensor goes off? How is the alarm assessed?

c. How do you plan to keep physical security performance up to standards? Perform regular audits, drills and provide training. Record incidents. Have a training log and updated access lists that are periodically reviewed. Assess whether the current system is working. Make sure staff know the proper procedures. Maintain security equipment and detection capabilities.

Notes: