SAND2012-8658P

Physical Security for Bioscience Laboratories

Instructor Guide

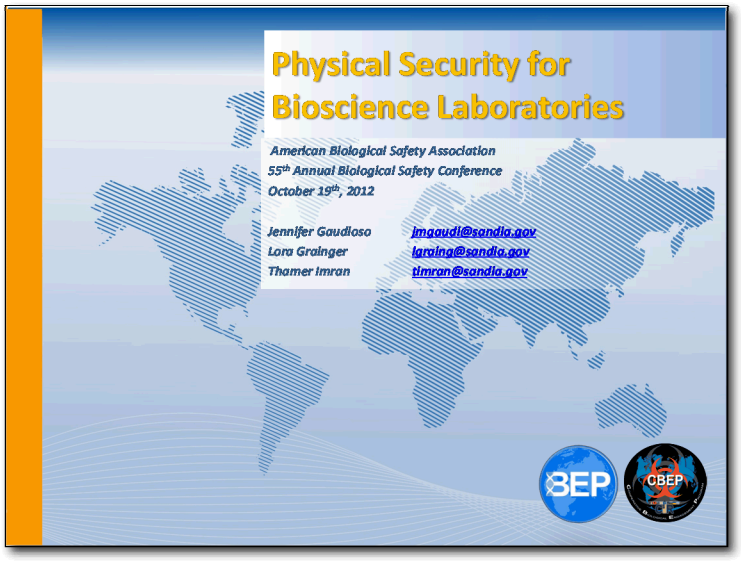
Sandia National Laboratories
International
BIOLOGICAL THREAT REDUCTION

BEP

CBEP
Cooperative Biological Engagement Program

Welcome & Introductions

Slide 1



Introduce Instructor(s):

[Introduce others associated with the training, as appropriate]

Name

Affiliation

Representation (I'm here on behalf of. . .)

Quick Experience Glimpse

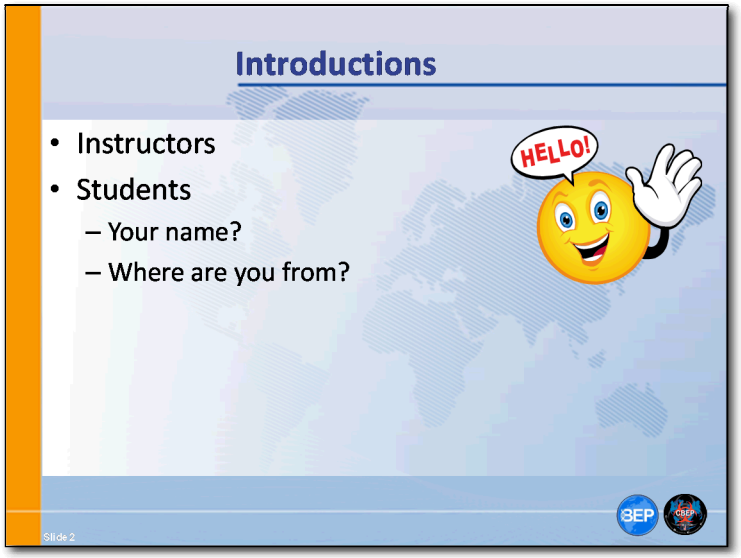
Relevancy of the Course to your experience

Welcome & Introductions

Before you introduce yourselves, I'd like to provide some reminders about this facility and the training:

1. Restrooms are . . .
2. Exits are . . .
3. Evacuation procedures are . . .
4. [any escort or restricted access procedures]
5. We will have intermittent breaks during the course, but please feel free (or not) to take a quick break if you need to at other times during the course
6. Beverages and snacks will be available at (time) and at (location). You may/may not eat and drink in this room
7. Please silence any cell phones or other noise-making devices.
8. Others . . .

Slide 2



Welcome & Introductions

Let's go around the room and let each of you introduce yourself. Please tell us your name, where you work (organization and/or title, as appropriate), and what you hope to gain from the course.

Ground rules

This will be a very interactive session and you will learn the most if you participate fully. We will not intentionally force any one to speak or to do an activity that embarrasses them – if you are uncomfortable, please speak to one of the leaders. For those of you who like to talk, please share your expertise but be aware of those around you who may be quieter and give them time to share their opinion as well. We ask that everyone respect the break times and report back promptly when asked to do so. But most of all, we want to make this a fun time to learn, so remember to smile and enjoy yourself!

Transition to Objectives

Goal

To review the Action Plan and Learning Objectives for the course and to solicit any additional learning goals from the participants.

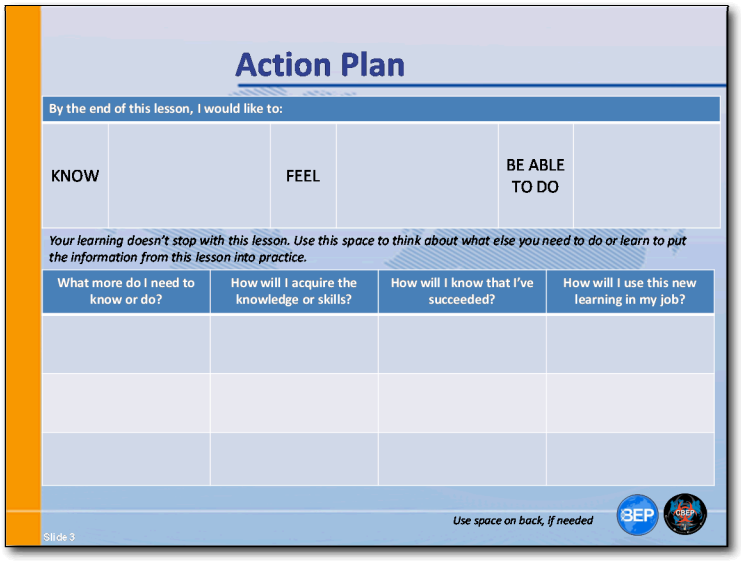
Time

20 minutes

Key Messages for Instructor

Welcome & Introductions

Slide 3

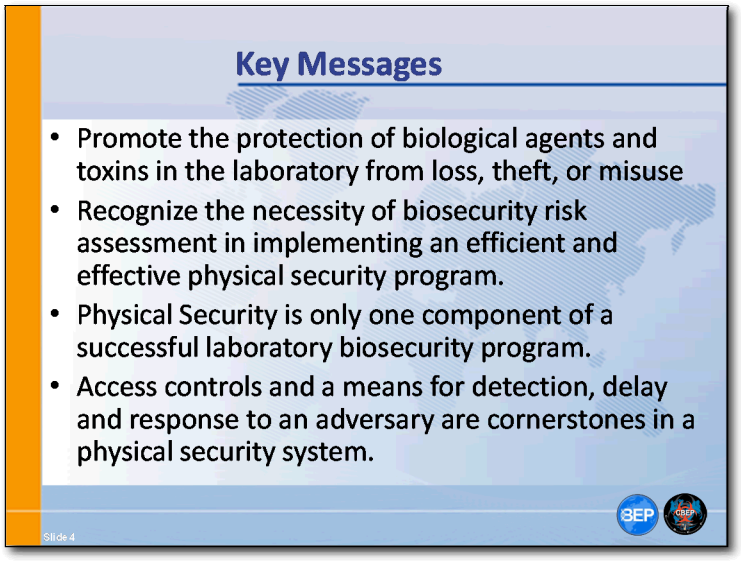


Instructions for the Action Plan handout:

- The Action Plan handout is on page __ of the student guide.
- It is designed to help you assess your learning of the material as we go through the course. It is also referred to as a learning contract.
- Go over each section of the Action Plan. . .
- The sections KNOW, FEEL and DO are designed to help outline personal learning objectives for this course.
- Ask each participant to think about what they would like to be able to KNOW, FEEL, and DO once this course is completed
- Tell the students that this is their own Action Plan. It does not need to be shared with anyone. It can be used during the course and after the course to help continually reach learning goals.
- Allow 5 minutes

Welcome & Introductions

Slide 4



Background Information for Instructor

Review the key messages, these can be read from the slide. Check for understanding and verify that these messages are consistent with student expectations.

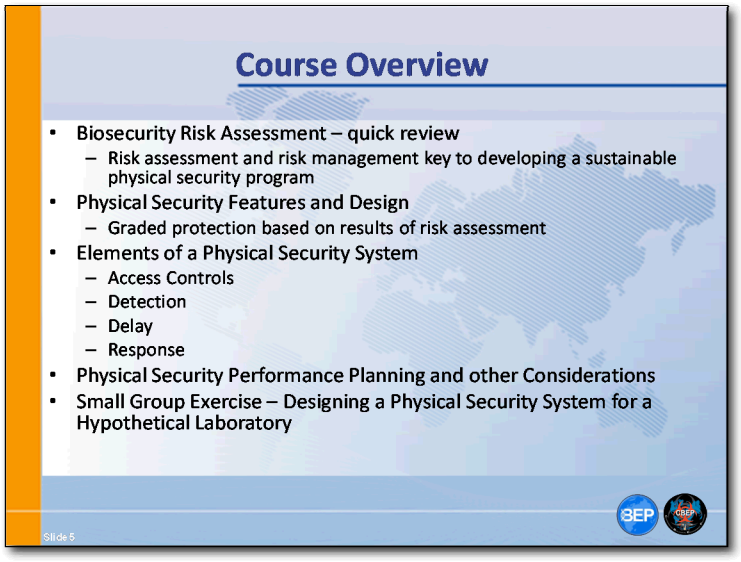
Capture any additional KNOW, FEEL, or DO or other learning goals

Capture any learning goals that will supplement course objectives and address any that are outside the scope of the course.

This course is flexible in nature. If there is a learning goal that is easily incorporated into the course, feel free to add it. Please note successful additions and consistently requested learning goals in the evaluation portion of this course and/or to GBRMC administrators.

Welcome & Introductions

Slide 5



Background Information for Instructor

This slide is a brief overview of the course.

Transition to Introduction to Physical Security – Risk Assessment

Introduction to Physical Security – Risk Assessment

Slide 6

Background Information for Instructor

Introduce the definition for Physical Security to the students.

In Plenary as the students for examples of Physical Security or for some things that are involved in a Physical Security System.

Expected Responses

- Perimeter Fencing
- Locks on Doors
- Guard Force
- Cameras
- Alarms

The students likely won't come up with the concept of how a risk assessment may tie in to physical security – this is a point we'd like to solidify. The specific steps of detect, delay and response as well as performance will also be new concepts.

A schematic of how these things fit together is shown on the next slide.

Introduction to Physical Security – Risk Assessment

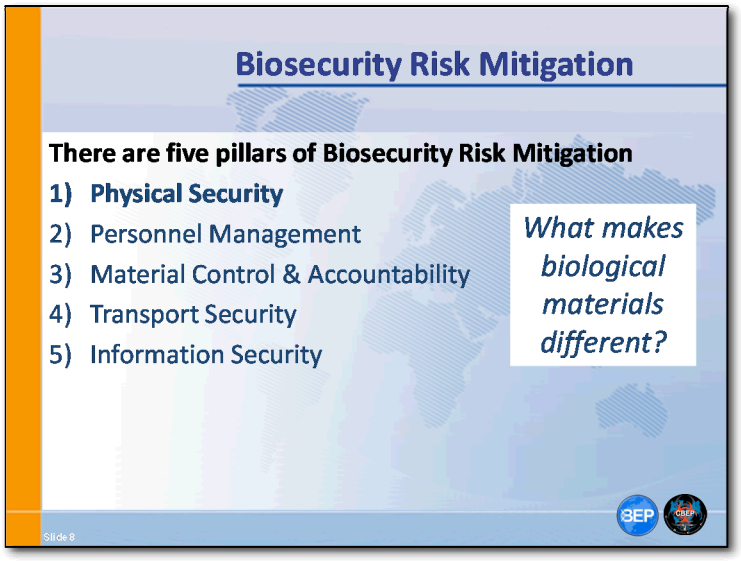
Slide 7

Background Information for Instructor

- Review the AMP model of Biorisk Management with the participants.
- Integration of laboratory biosafety (protect people from pathogens) and laboratory biosecurity (protect pathogens from people)
- These points will be discussed throughout the course as they come up in the material.
- A complete physical security system will address AMP and each of these points will be discussed throughout the course as they come up in the material.

Introduction to Physical Security – Risk Assessment

Slide 8



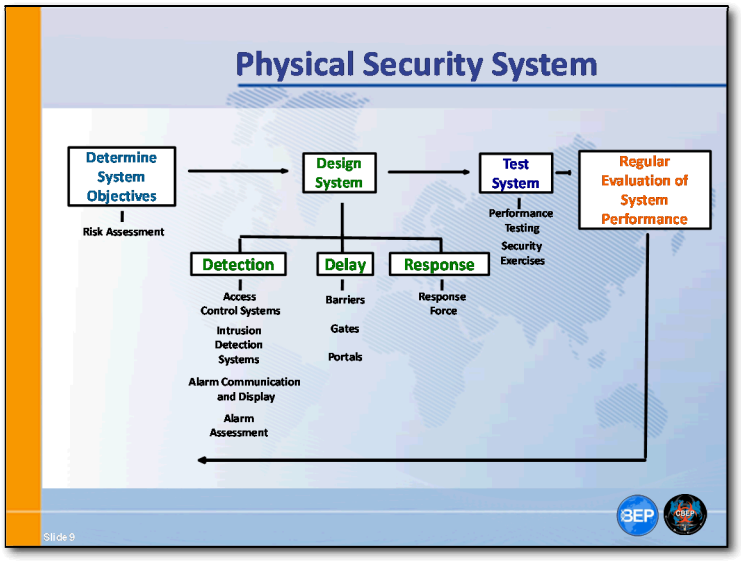
Background Information for Instructor

This slide is used to orient the students to how physical security fits into an overall biosecurity risk mitigation plan. Today we will only focus on physical security.

Keep in mind that because of the unique properties of biological materials (can replicate, spread, infectious) that the physical security of a laboratory may differ from the physical security of a nuclear facility. Although there are some similarities.

Introduction to Physical Security – Risk Assessment

Slide 9



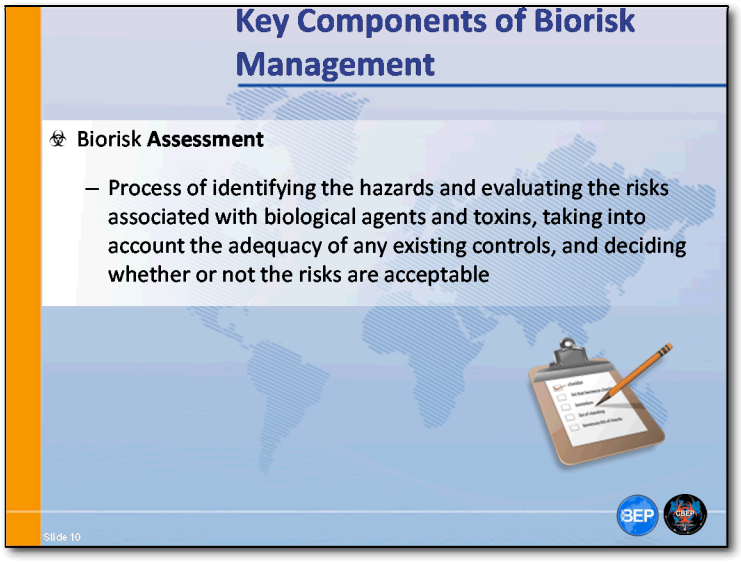
Background Information for Instructor

This slide is also a brief overview of the course but in schematic form. The course will cover the topics listed. A complete physical biosecurity system is a combination of all of the items listed above.

The overall goal is to achieve the desired performance as defined by the system objectives. This follows a process of systematic system design, testing the system, and then providing regular performance maintenance to the system. It should be noted that depending on the situation, the means to achieve the system objectives may rely on either low or high technology.

Introduction to Physical Security – Risk Assessment

Slide 10



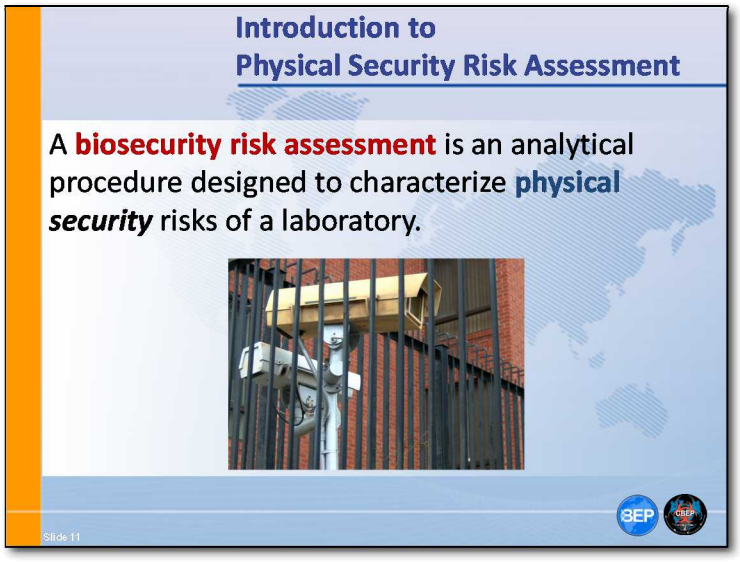
Background Information for Instructor

The first step in the process of determining what features of a physical security system are necessary is a thorough risk assessment.

In this case we are not as concerned with the hazards as we are the threats to the assets contained in the laboratory. The risk assessment should take into account any existing means of physical security in order to decide if additional controls are necessary.

Introduction to Physical Security – Risk Assessment

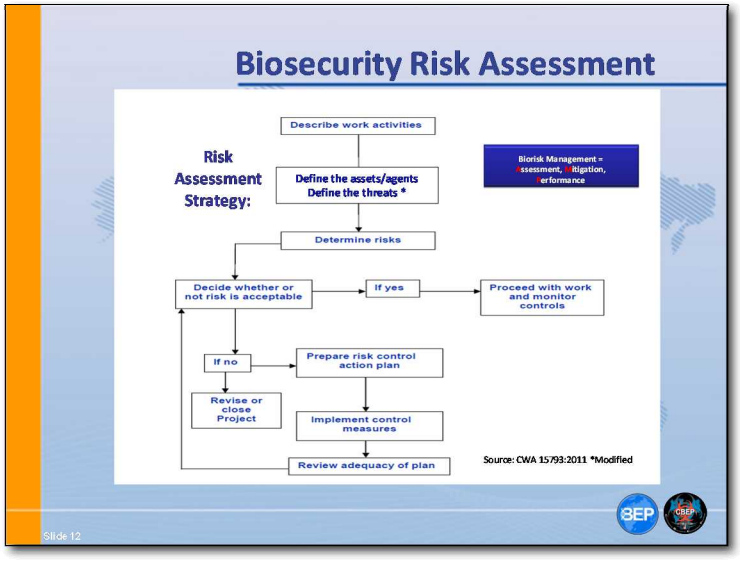
Slide 11



Background Information for Instructor

This series of slides describes, what is included in a physical security risk assessment.

Slide 12



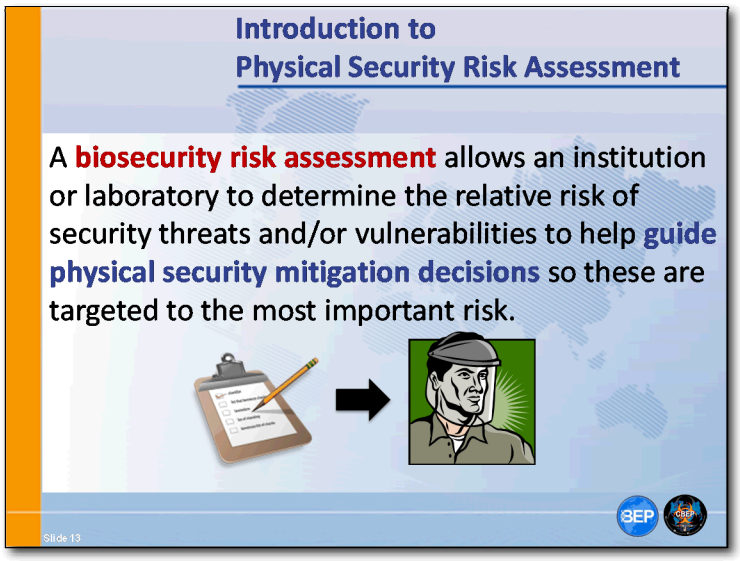
Introduction to Physical Security – Risk Assessment

Background Information for Instructor

This is a modified version of the process follow from the CWA15793. The difference is the specific defining of the assets/agents and threats for security. The original process just asks to define the hazards. This process is the one the students will use in this course

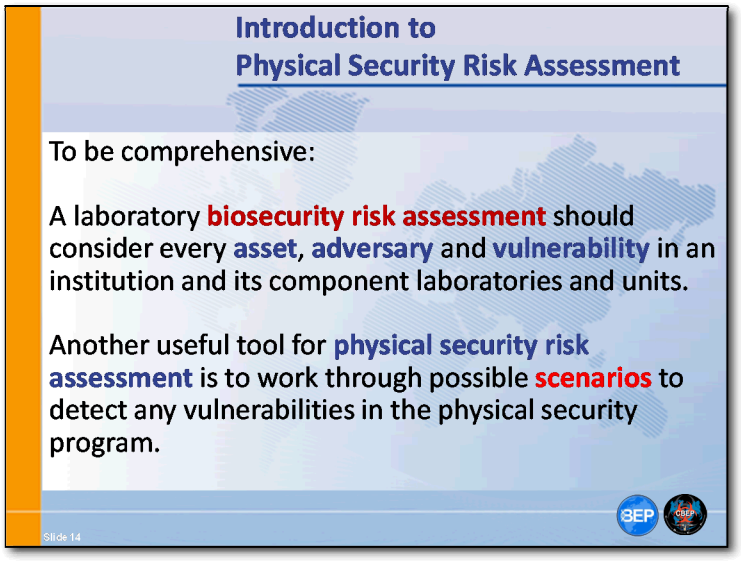
Walk through this flow chart, from the CWA 15793:2011, that is used as a strategy to assess risk. Highlight the progression of identifying the assets/agents and defining the threats to deciding whether the risk is acceptable or not and what to do in either case.

Slide 13



Introduction to Physical Security – Risk Assessment

Slide 14



Background Information for Instructor

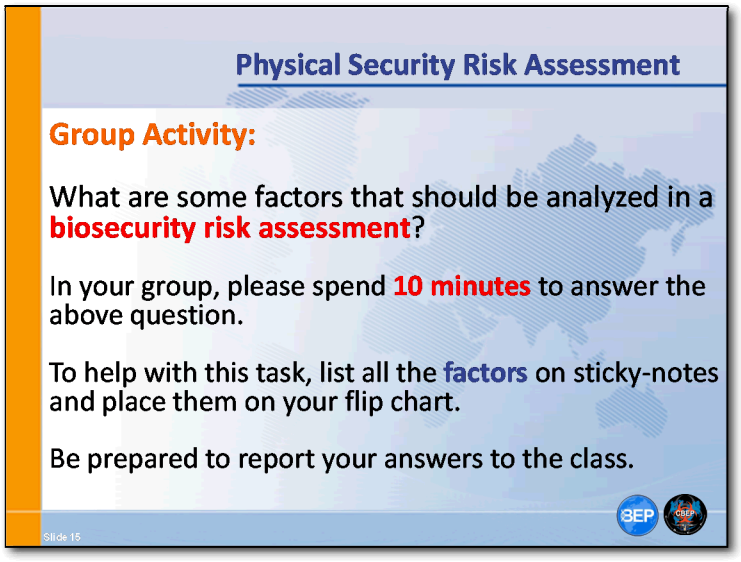
Determining the laboratory assets in terms of potential adversaries, vulnerabilities and a particular scenario is a way in which physical security risk can be assessed.

In plenary ask the students:

What are some factors that could be considered in the risk assessment?

Introduction to Physical Security – Risk Assessment

Slide 15



Small group activity (15 minutes).

Activity Instructions (to students)

1. In your group, please spend 10 minutes to answer the question "What factors should be considered in a physical security risk assessment?
2. To help with this task, list all the factors on sticky-notes and place them on your flip chart.
3. Be prepared to report your answers to the class.

Introduction to Physical Security – Risk Assessment

You have 15 minutes to complete this activity

Directions for Instructor:

- After 10 minutes, ask the students to students to stop working on the exercise
- Spend a few minutes reviewing some of the factors the students came up with.
- If time allows, have the students categorize the factors they identified
- Then in association with the next slide, group the factors within each category into factors affecting either likelihood or consequences.
- Generally, the expected responses will fall out into five major categories: a. Agent Properties b. Laboratory Infrastructure c. Human Factors d. Operational Factors e. Environment and Community Factors.

Introduction to Physical Security – Risk Assessment

Expected Responses

These are the expected responses. The factors are in the bullet points under each category heading. The un-bolded points are factors that would most affect likelihood and the **bolded** points are factors that would most affect consequences. Note: There will be some variation of these answers, especially when comparing the affects on likelihood and consequences.

Asset/Agent Properties:

- **Pathogenicity / Virulence**
- **Infectious Dose**
- **Potential Outcome of Exposure**
- Potential Routes of Infection
- Stability of the Agent in the Environment
- **Morbidity / Mortality**
- **Availability of Therapeutic Interventions**
- **Ease of dissemination**

Laboratory Infrastructure:

- Locking Doors
- Open Windows
- Public Access
- Alarm systems
- Security Cameras

Human Factors

- Susceptibility to corruption
- Level of Training
- Workload and Fatigue
- Access to assets/agents

New Responses from Students:

Introduction to Physical Security – Risk Assessment

Expected Responses

Operational Factors

- Good Laboratory Practices
- Material Control and Accountability
- Transport Security
- Information Security
- Proper Decontamination
- Waste Management
- Other Administrative Controls

Environment and Community Factors:

- **Presence of the Agent in the Environment Around the Laboratory**
- **Immune Status of the Community**
- **Population Density of the Community**
- **Presence of Suitable Hosts or Vectors**
- **Economic status**
- Public Perception

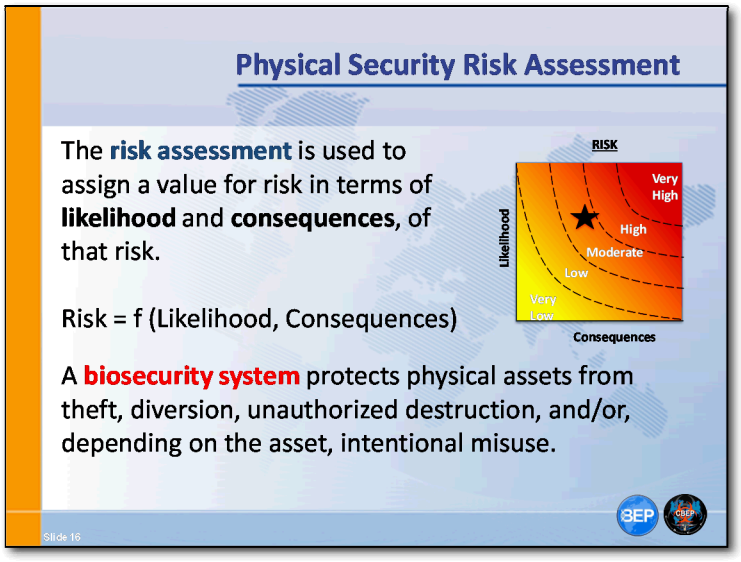
Adversary Characteristics

- Motive
- Means
- Opportunity
- Drive

New Responses from Students:

Introduction to Physical Security – Risk Assessment

Slide 16



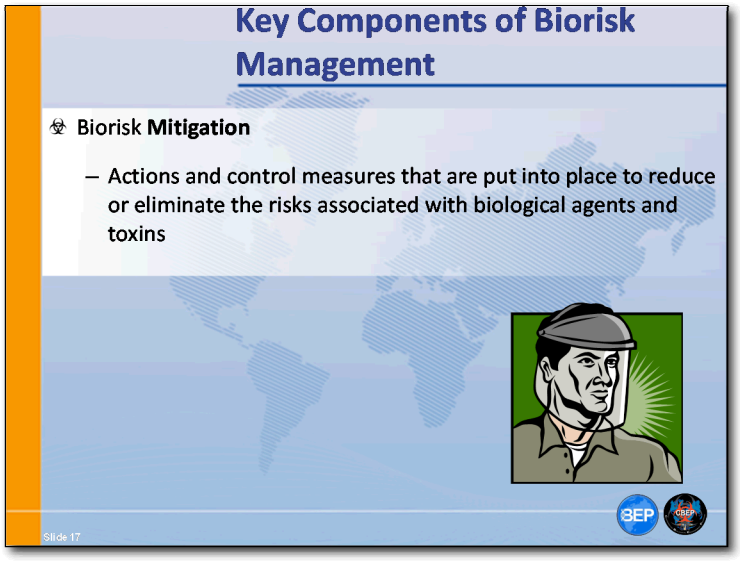
Background Information for Instructor

After reviewing this slide have the students review the factors that they identified in the previous activity and have them identify the factors that contribute to likelihood and consequences.

Transition to Physical Security Features and Design

Physical Security Features and Design

Slide 17



Background Information for Instructor

Now we are transitioning to the mitigation portion of physical security. This includes a discussion on the theory, design and physical security risk mitigation mechanisms.

Slide 18

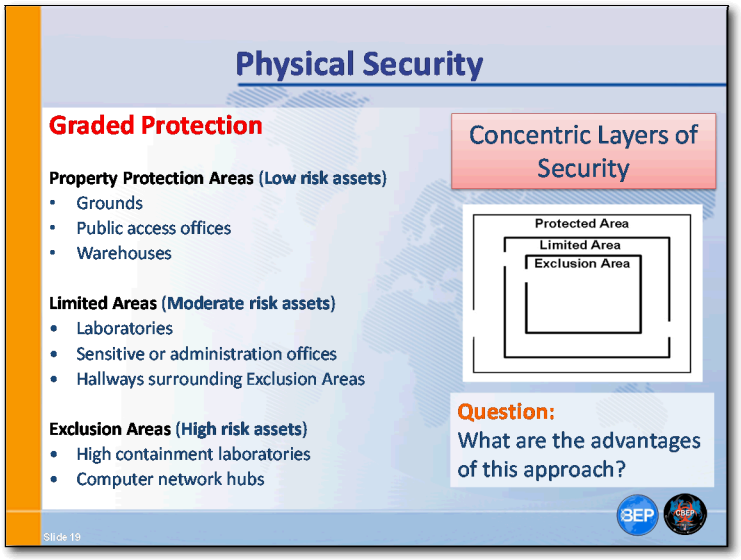
Physical Security Features and Design

Background Information for Instructor

This is a review slide to bring the class back into focus for the next portion of the course.

In bioscience facilities, the most important assets may be biological organisms, dual-use equipment, instruments, chemicals, computers, or files, for example.

Slide 19



Physical Security Features and Design

Background Information for Instructor

Increasing security incrementally and forming concentric layers of protection around the facility's agents based on the results of the risk assessment achieve a graded protection system.

Graded protection also helps ensure effective use of resources and unnecessary impact on the bioscience institution's mission. The layer within which an asset resides should correspond to the level of security it requires.

Keep in mind that the overall layout of the facility and the locations of access control features to access the inner layers of the physical security system are important to consider in order to ensure that the normal and emergency paths of employees and visitors do not inadvertently leave gaps in security boundaries. This includes keeping a close eye out for common travel routes are enforced without providing alternate, unsecured routes, and that emergency egress paths do not channel individuals into areas to which they would not normally have access.

Boundaries may be established to demarcate the areas that are under some sort of access limitation. Note, that depending on the risk assessment, marking boundaries may also contribute to risk by acting as an indicator of where assets are located. Examples of boundary demarcation include:

- A fence defines the boundaries of the campus as well as provides a means to control personnel and vehicle access.
- Use of signs.
- Boundaries to restricted areas can include walls, windows, doors, pass-through boxes, pass-through autoclaves, or other equipment access points.

Physical Security Features and Design

Background Information for Instructor

Each inner layer should have additional elements of security built in compared to the outer layer. For the inner most layer would include additional physical security, personnel security, and MC&A requirements than the next outer layer. Keep in mind that information and transportation security requirements, may also be included, but are more likely to vary based on the need identified in the risk assessment.

The nested levels of protection are referred to as “Property Protection Areas,” “Limited Areas,” “Exclusion Areas,” and “Special Exclusion Areas.” Limited, Exclusion, and Special Exclusion Areas are always considered to be restricted areas as the term is used in the preceding sections.

Keep in mind that the strength of the perimeter envelope protecting a restricted area will influence how long it takes an outside adversary to gain unauthorized access to the restricted area.

- The stronger the perimeter is, the longer the “delay” will be between the time of the initial intrusion alarm and the time at which the outside adversary can gain access to the protected material.
- The longer the delay, the more opportunity the response force has to respond to an intrusion detection alarm.

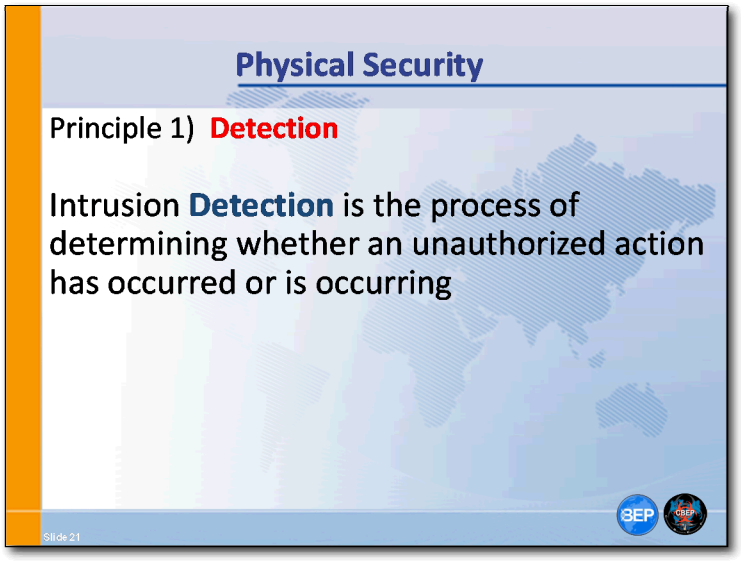
Physical Security Features and Design

Slide 20

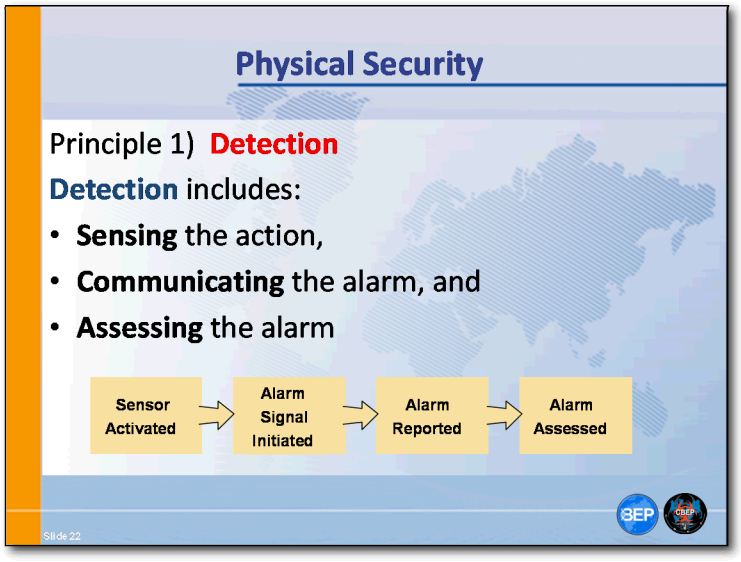
Transition to Detection, Delay and Response

Detection, Delay and Response

Slide 21



Slide 22



Detection, Delay and Response

Background Information for Instructor

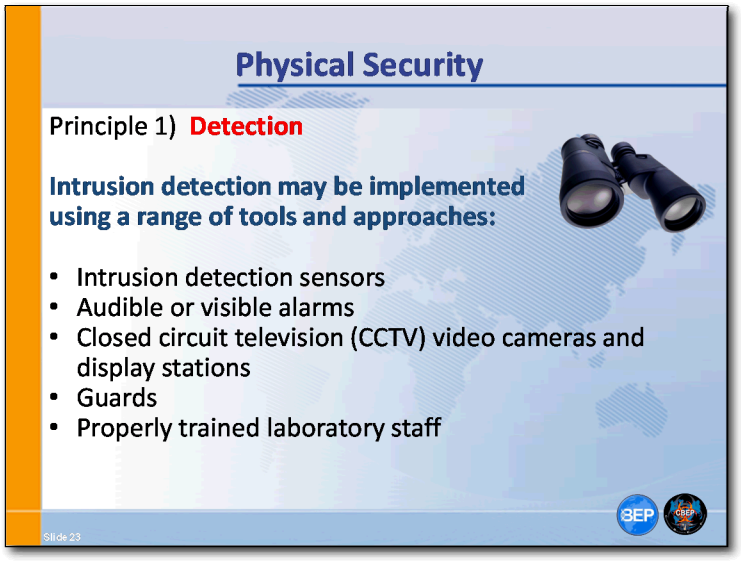
Intrusion detection systems alert security personnel to attempts to gain access without authorization. The detection aspect of physical security has many components that allow the process to work as a whole. In this context, we'd like to extend our definition of detection to also include an assessment stage where after the sensor is activated, the alarm signal is initiated, then the alarm is reported that the alarm is assessed to determine the nature of that change in status.

In its simplest form, intrusion detection is an alert staff member who notices that something is amiss, such as a broken window or an open door that is normally closed. In more advanced forms electronic intrusion detection devices send alarm signals to a central monitoring station. Alarms must then be assessed to determine whether they are valid or are false alarms. Valid alarms that have been assessed as either an attempted or successful access to a restricted item or area by an unauthorized individual should be addressed by properly trained response personnel.

Mechanically based systems are inherently less effective than electronic systems but, depending on the facilities' level of risk tolerance and local regulations, can be used when electronic systems are too costly or are not available. The advantages of electronic intrusion detection devices include an audit trail of activity, whereas strictly mechanically based systems do not have this capability and must rely on other means such as additional personnel or procedures.

Detection, Delay and Response

Slide 23



Detection, Delay and Response

An example of some components of the detection process are listed below:

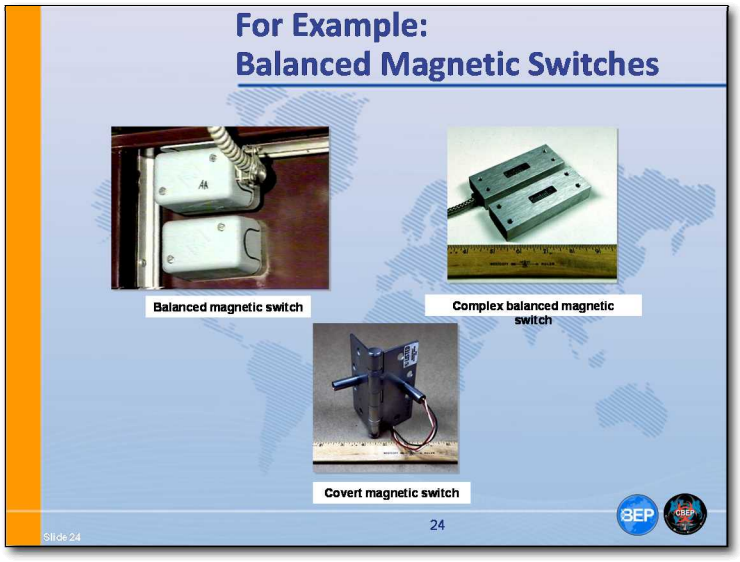
- Motion sensors, cameras (with adequate lighting), seals, strong door, no windows, guard patrols, electronic intrusion detection systems (with constant monitoring)
- If forced entry occurs, or if a door or other monitored entryway is open for an extended period of time, an alarm will be generated.
- The electronic network can be configured to detect tampering so that if a communication line is cut or a junction box is tampered with, an alarm will be generated under these conditions as well.
- Glass-break sensors will send an alarm if a protected window is broken. Motion detection may also be utilized to generate an alarm.
- Doors to pass-through autoclaves or equipment/maintenance crawl spaces that are large enough for a human to navigate should also be secured and alarmed as appropriate.

It should be noted that other sensor type not associated with detecting a breach in the boundary of the restricted area, but within the area itself, often require additional procedural actions in order to ensure they do not alarm during normal daily activities.

- These types of sensors, unless used in areas where personnel are not usually present, can be configured to a “by-pass” mode during normal business hours, and activated only upon close of business in the area where they are located.

Detection, Delay and Response

Slide 24

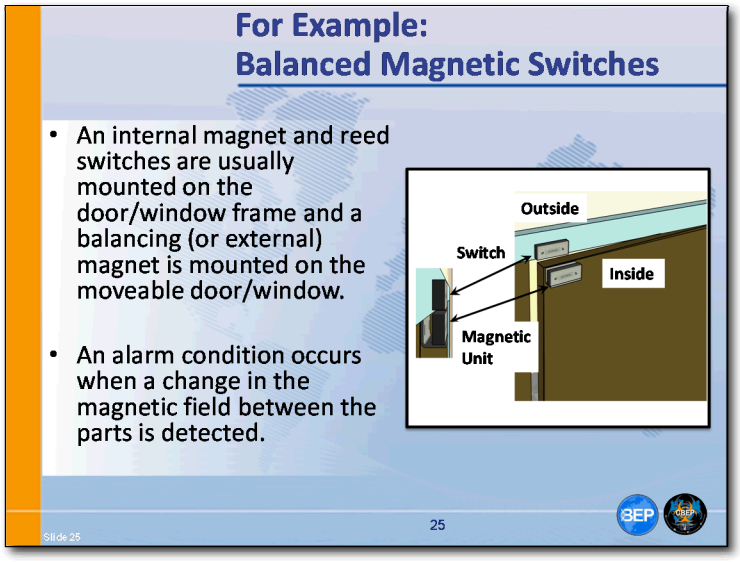


Background Information for Instructor

There are many varieties of balanced magnetic switches that vary in their complexity and applications. Some use multiple magnets and some even have internal electromagnets for self-testing. Manufacturers have been able to reduce tamper vulnerability by using a variety of magnets in different configurations, magnetic shielding material, creating standoff distances, and also adding tamper indicators.

Detection, Delay and Response

Slide 25



Background Information for Instructor

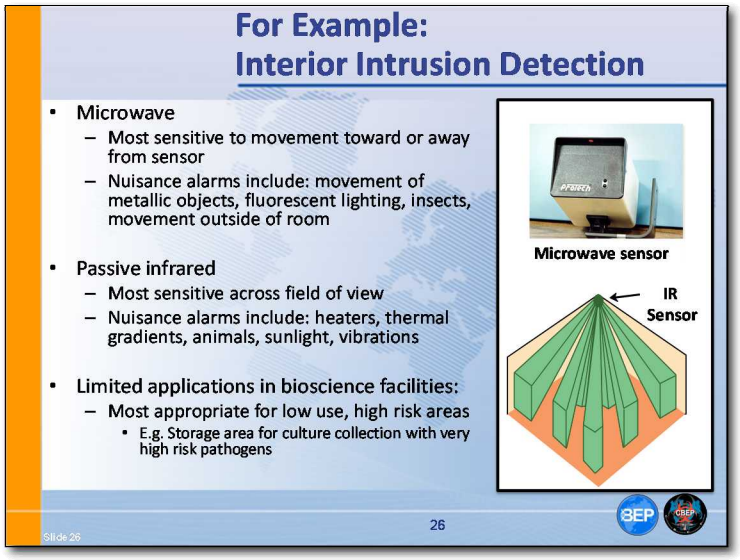
The balanced magnetic switch is used for both door and window protection. Generally, a change of the magnetic field between open and closed positions triggers the alarm. This type of protection is fairly inexpensive compared to other detection methods. It also requires more skill to defeat.

Major Causes for Nuisance Alarms:

- Poorly fit doors or windows
- Improper installation
- Extreme weather conditions which cause excessive movement of the door or window

Detection, Delay and Response

Slide 26



Background Information for Instructor

Microwave sensors detect motion through disruption of the microwave energy. The sensor can distinguish the energy frequency that it emits compared to the energy frequency that it receives. If there is a difference greater than a pre-set threshold, the system will alarm. It can detect movement toward or away from the sensor better than movement across the detection field. This should be taken into consideration in security design.

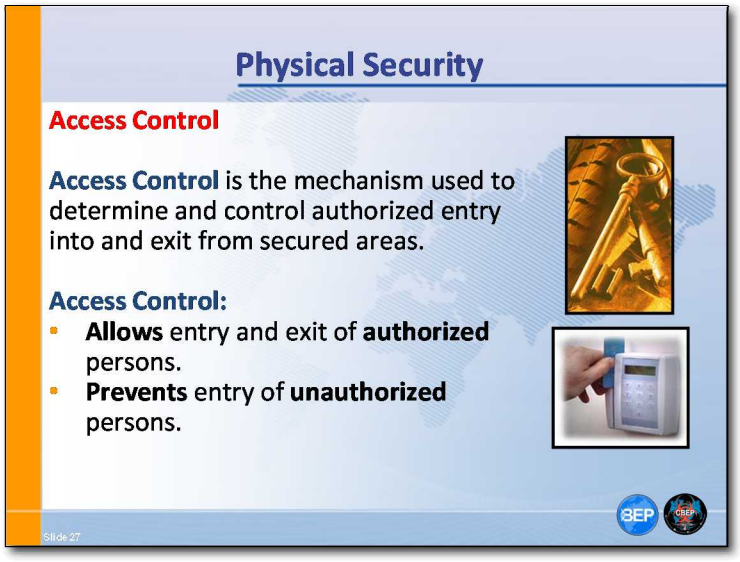
Passive infrared sensors are the most commonly used volumetric sensors indoors. They detect changes in thermo radiation by comparing temperatures of an object compared to the ambient background temperature. They require a line of sight to be effective.

Lecture

Many of the components listed under detection also serve to delay an intruder from accessing assets so that the adversary can be detected, assessed and responded to.

Detection, Delay and Response

Slide 27



Background Information for Instructor

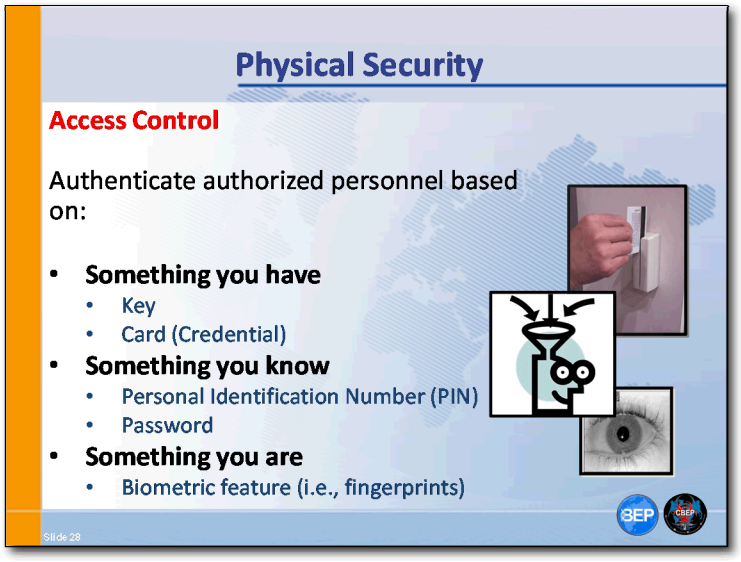
Access control mechanisms include locks and other barriers to prevent unauthorized individuals from gaining access to restricted items or areas. The type of access controls selected depends on the level of surety required that only authorized personnel can enter a restricted area, which will be based on a risk assessment.

It should be noted that for access controls to be effective, valuable biological materials should only be stored and used in areas appropriate to the level of risk they pose, and only authorized personnel should be allowed access to those areas.

Administrative controls can enhance access controls by providing standard operating procedures for visitors and/or escort policies, as well as with maintaining access records.

Detection, Delay and Response

Slide 28



Background Information for Instructor

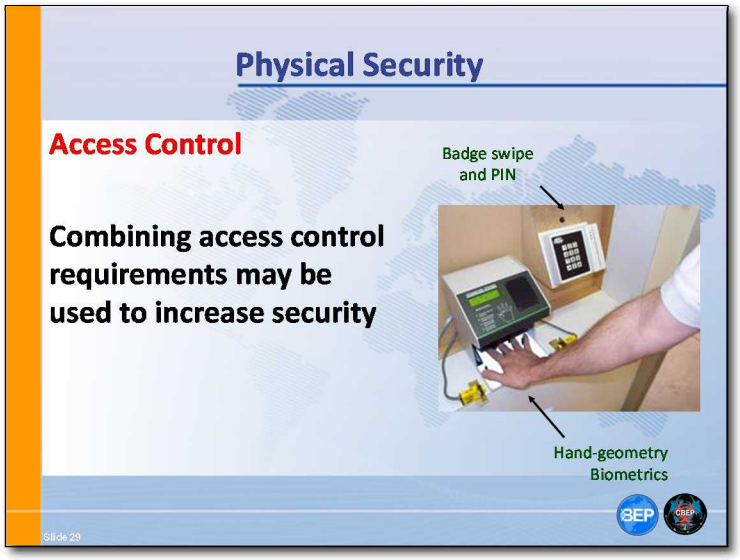
There are many ways to grant access. For example, it can be based on the following criteria:

1. Something you have – Key, card, unique item
2. Something you know – password, pin – this ensures that the individual who possesses the first item is authorized to possess it.
3. Something you are – biometric feature such as fingerprints, eye scan.

Note that all intrusion detection and access control measures should be capable of providing an audit trail.

Detection, Delay and Response

Slide 29



Background Information for Instructor

In plenary ask the students to identify some advantages and disadvantages to different types of access controls.

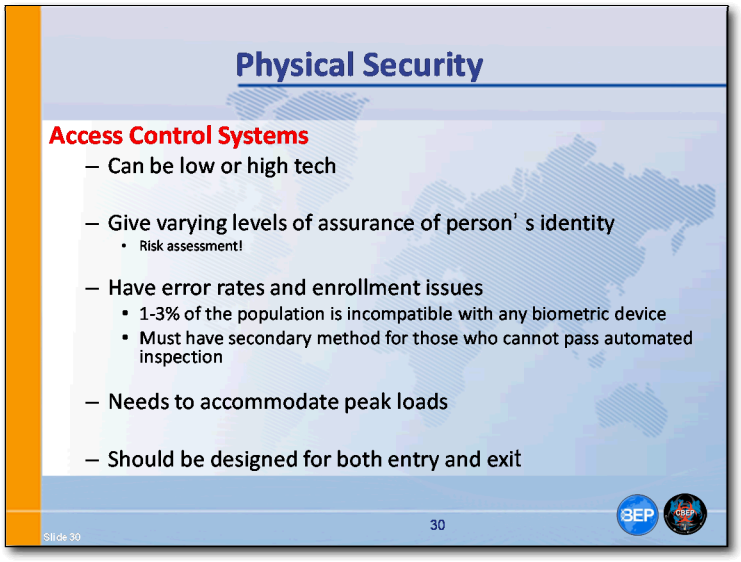
Expected Responses:

Generally, these are the factors that should be considered with each access control: (specifics are in notes section of slide)

Expense, ease of use, ease of misuse, ease of operation, validity, technical capabilities, maintenance, redundancy with other access control,

Detection, Delay and Response

Slide 30

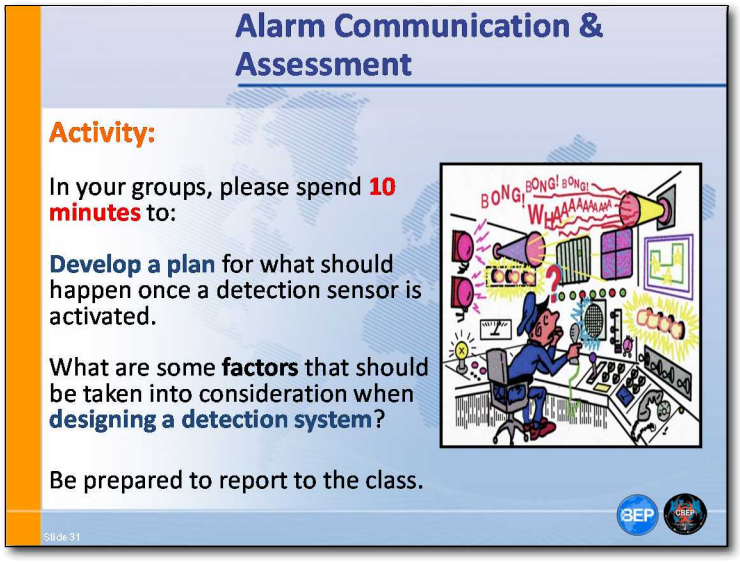


Background Information for Instructor

This is a review slide for access controls.

Detection, Delay and Response

Slide 31



Small group activity (15 minutes).

Activity Instructions (to students)

- You have 10 minutes, in your groups, to develop a plan for what should happen once a detection sensor is activated and to also list some factors that should be taken into consideration when designing a detection system.
- Be prepared to report to the class.

Detection, Delay and Response

You have 10 minutes to complete this activity

Directions for Instructor:

- After 10 minutes, ask the students to stop working on the exercise
- Lead a 5-minute plenary discussion. Begin by asking for one group of students to report their answers.
- Continue around the room, asking other groups to report out, as time allows.

Be sure to highlight any similarities, differences or unique answers.

Detection, Delay and Response

Expected Responses

Develop a plan: Should include aspects of the following and how they could be achieved.

- **Sensing** the action,
- **Communicating** the alarm, and
- **Assessing** the alarm

Factors for designing a detection system

- Cost
- Detection method/applicability
- Nuisance alarms
- Location
- Maintenance
- Training
- How to determine the cause of the alarm
- Who and how the alarm is assessed
- SOPs

New Responses from Students:

Ask: Any questions about Detection and Access controls?

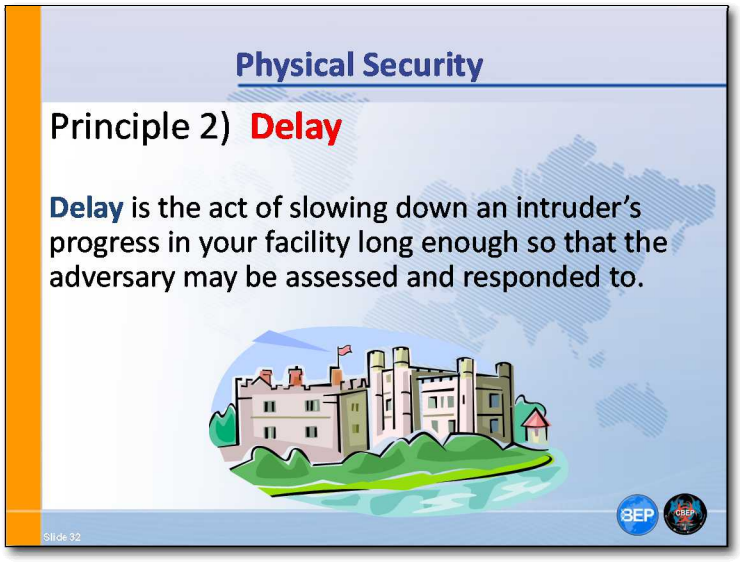
- Take a Break (10 minutes)

Time Check

- You should be approximately __ hour and __ minutes into the course. You have __ hours of the course remaining.

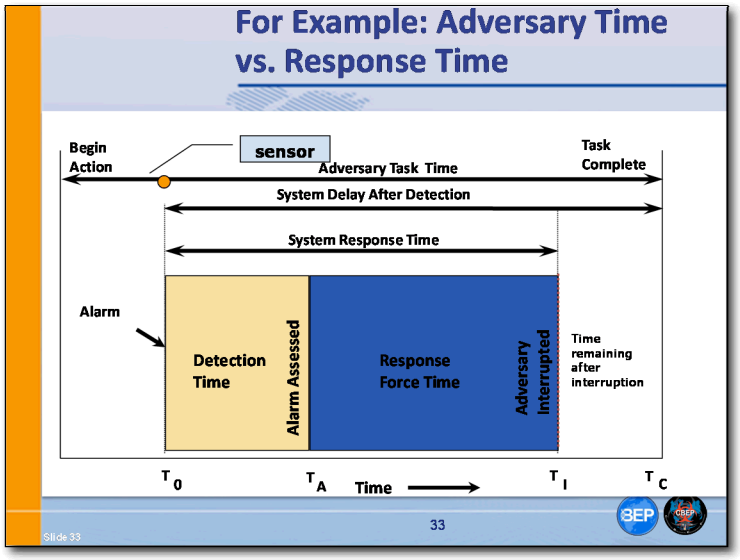
Transition to Delay

Slide 32



Detection, Delay and Response

Slide 33



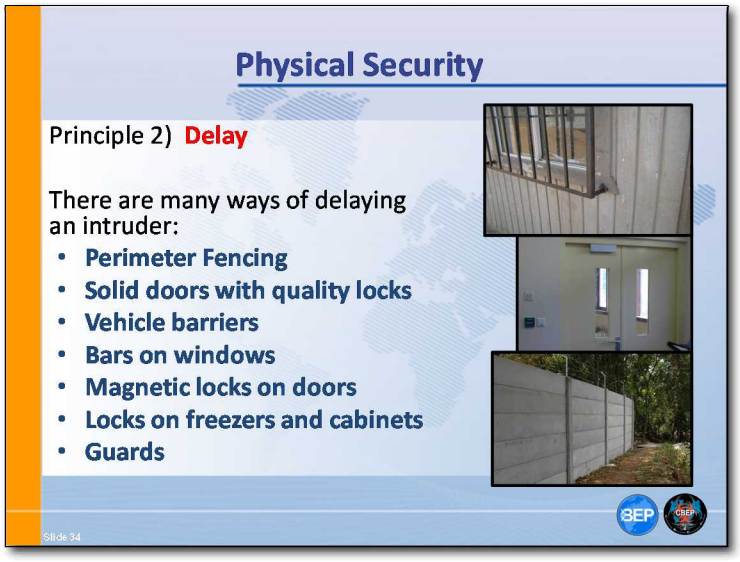
Background Information for Instructor

Not delay so that you can be detected – this is important especially for physical security system design. The response time must be less than the adversary task time remaining after detection.

What can you do to increase adversary task time? Using delay mechanisms.

Detection, Delay and Response

Slide 34



Background Information for Instructor

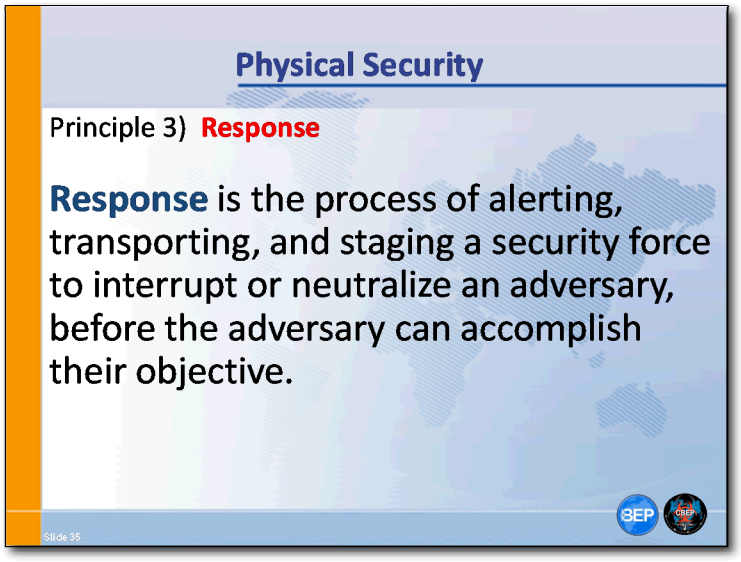
In order to **delay** intrusion, a security system may employ gates and fences, walls, barred windows, heavy doors, long corridors, and high quality locks and access controls. The various ways of delaying an adversary should be based on a thorough risk assessment.

Ask: Any questions about Delay?

Transition to Response

Detection, Delay and Response

Slide 35



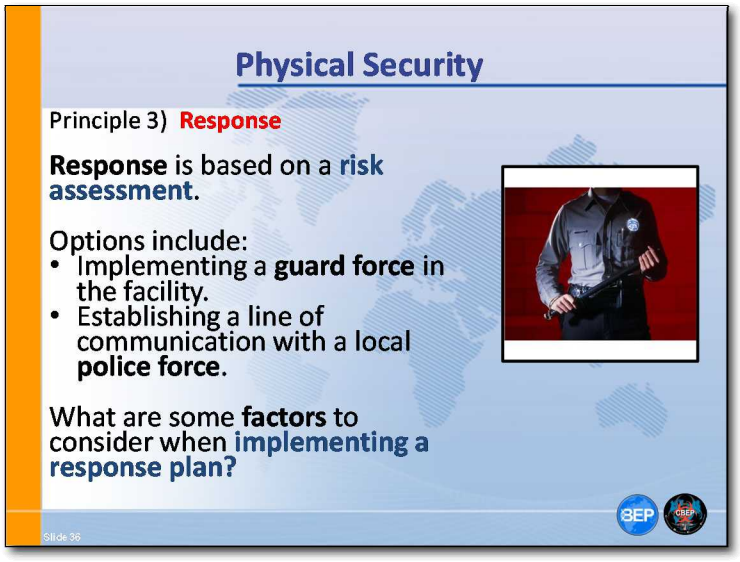
Background Information for Instructor

Response is tied to the overall system objective

- **Deny**: To prevent an adversary from reaching the target/objective
- **Contain**: To 'catch' an adversary before they leave with the target or before they accomplish the objective

Detection, Delay and Response

Slide 36



Background Information for Instructor

On-site guard force

- Can serve intrusion detection and alarm assessment roles in mechanically-based physical security systems
- Supports electronic systems:
  - Monitors Alarm Communication & Display (AC&D) system
  - Assesses electronic alarms at alarm console or at alarm location
- Patrols perimeter and buildings
- Summons and directs local law enforcement

Local law enforcement (police)

- Reinforces on-site guard force
  - Responds according to plan when summoned
  - Equipped and authorized to confront adversary

Detection, Delay and Response

In plenary, ask students:

What are some factors to consider when implementing a response?

Expected Response:

Qualification and training of responders

Enforcement responsibilities and skills

Equipment familiarity and training

Familiarity with facility features and operations

Knowledge of restricted area access and biosafety

Guard Force Post Orders

List specific duties and limits of authority

Procedures for response to specific alarm conditions

Emergency response procedures

Notification list

Memorandum of understanding with local law enforcement

Specific instructions and agreements

On-site training and orientation

Detection, Delay and Response

Background Information for Instructor

If the alarm sounds and the threat is assessed to be valid, a response to the situation must be made to try to apprehend the intruder. A response may come from a security guard force or a call may be made to the police. Only authorized personnel should try to handle an encounter with an intruder. Unauthorized personnel should be actively discouraged from trying to apprehend intruders. If necessary that individual should summon either on-site security personnel or local law enforcement to respond. Included in the response stage is an inherent recovery stage that gets the institution back to working conditions, incorporating any lessons learned during the security breach.

It should be noted that equipment malfunctions, accidents, and even animals can be the source of a suspected intrusion, and none of these occurrences warrant an official security incident response.

Records should be kept on each actual and each false or nuisance alarm. Each record should contain the date and time of the alarm, the cause of the alarm, or a probable cause if a definite cause cannot be established, and the identity of the recorder or the operator on duty and actions taken, if any. Analysis of these records can indicate what corrective measures need to be taken to minimize the false-alarm rate and can also indicate pattern of penetration testing.

Background Information for Instructor

Incorporating your risk assessment data will help to find the appropriate mitigation effort, with regard to response. It is important to consider the factors that may contribute to a breach in physical security, including local conditions and facility infrastructure.

Ask: Any questions about Response?

Take a Break (10 minutes)

Detection, Delay and Response

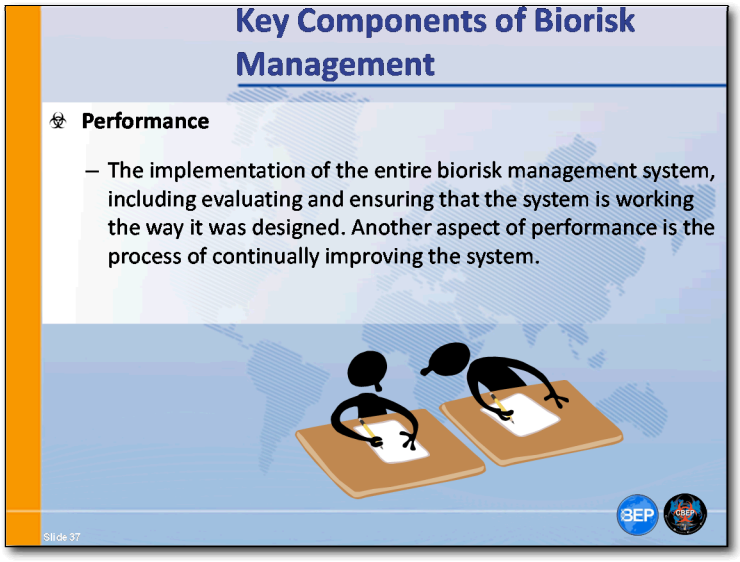
Time Check

You should be approximately __ hour and __ minutes into the course.
You have __ hours of the course remaining.

Transition to Physical Security Performance

Physical Security Performance

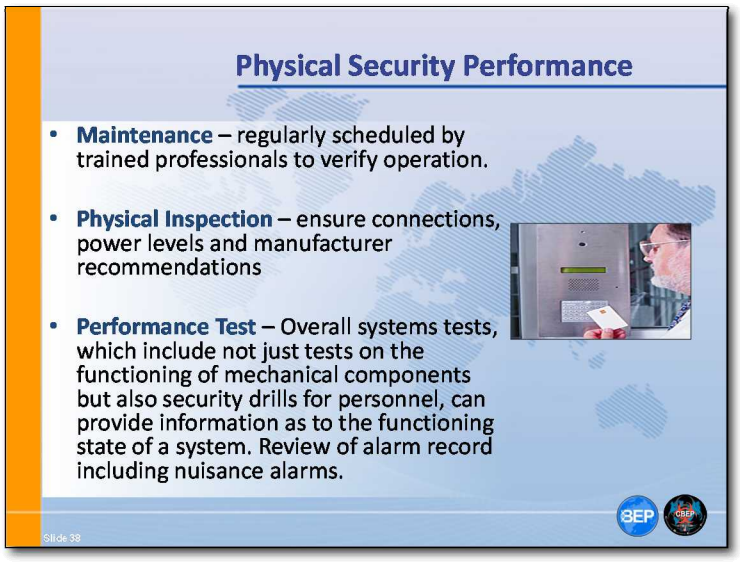
Slide 37



Background Information for Instructor

Next we'll spend some time reviewing aspects of Physical Security performance.

Slide 38



Physical Security Performance

Background Information for Instructor

Maintenance Plans can also be combined with **Performance Plans**, which ensure a system as a whole is performing as designed and/or as required.

Background Information for Instructor

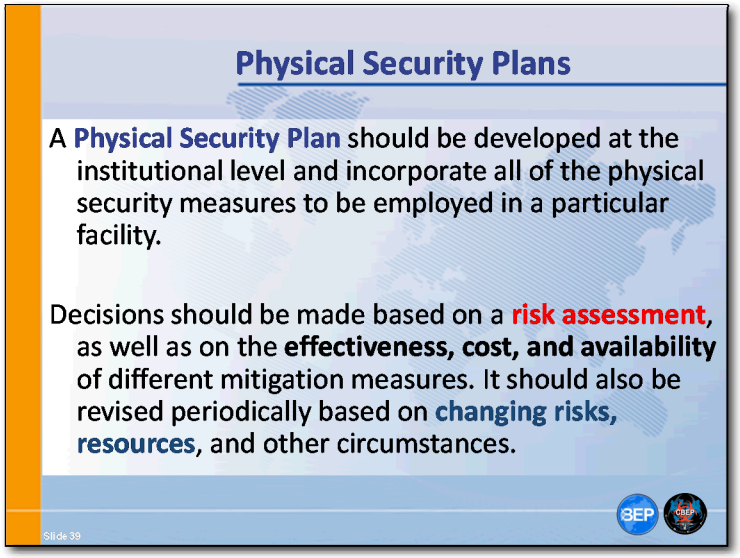
Security equipment, like other laboratory equipment, can be maintained by laboratory workers or professionals such as technicians employed or licensed by the manufacturer.

Question: What are some benefits and drawbacks of maintaining security technicians on staff? Of relying in outsiders?

Expected response:

Risk of insider threat.

Slide 39



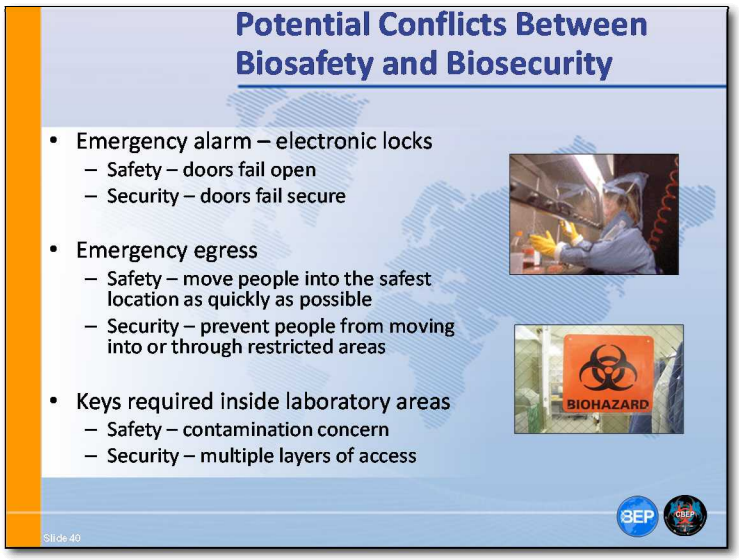
Physical Security Performance

Background Information for Instructor

Implicit in security is the concept of **balance**. For example, one should not spend a lot of effort securing the doors of a ground level laboratory if its windows are left completely unprotected.

Put another way, a secure area should be protected in its entirety at a consistent level. For example, an area is only as secure as its weakest entry/exit point or a camera is only as good as the person watching it

Slide 40



Physical Security Performance

Background Information for Instructor

Laboratory Biosafety

Objective: reduce or eliminate accidental exposure to or release of potentially hazardous agents

Laboratory Biosecurity

Objective: protect biological agents against theft by those who intend to pursue bioterrorism or biological weapons proliferation

Common strategy

Implement graded levels of protection based on a risk management methodology

Control of certain biological materials is necessary, but *how* that is achieved must be carefully considered

Biosecurity and biosafety should be integrated systems that avoid compromising necessary infectious disease research and diagnostics

Laboratory biosecurity supports the laboratory biosafety agenda of preventing disease in people, animals, and plants and minimizing the risk of worker injury

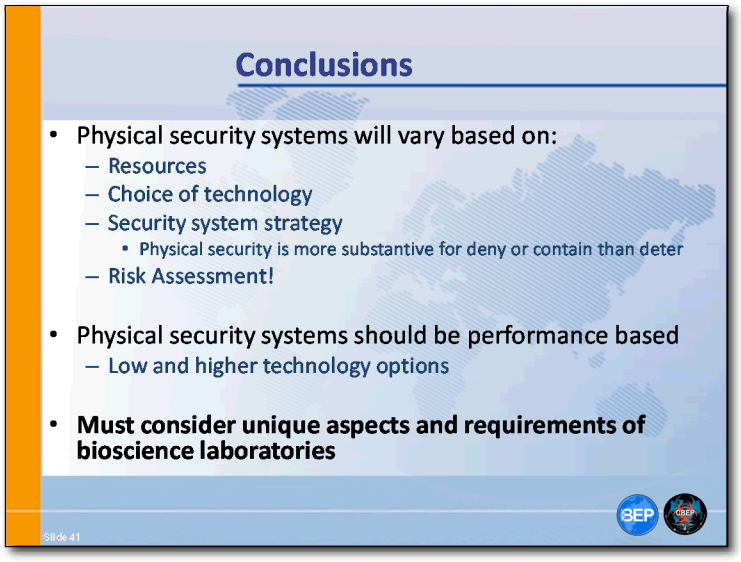
Limits the number of individuals who may be exposed to the hazards

Limits access to those who are professionally qualified and properly trained to be there

Access control procedures and records can be used to support investigations of laboratory safety or security incidents

Physical Security Performance

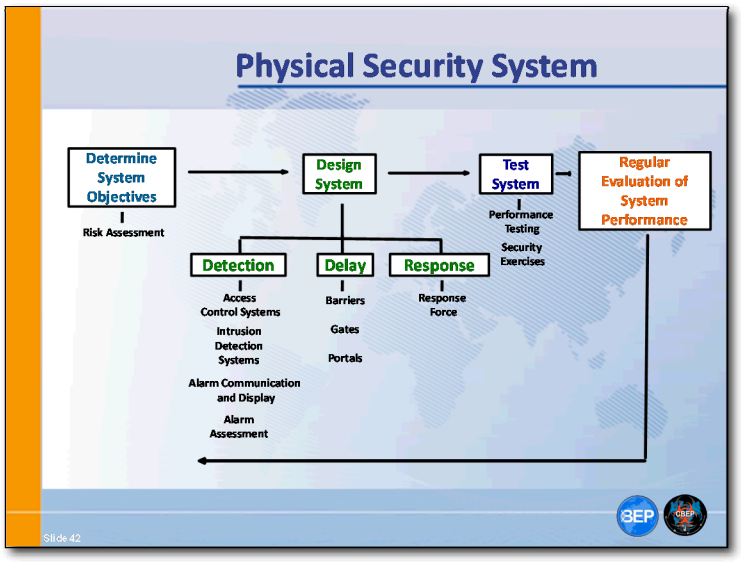
Slide 41



Background Information for Instructor

These next two slides are meant as a review of the key messages of the course.

Slide 42



Physical Security Performance

Background Information for Instructor

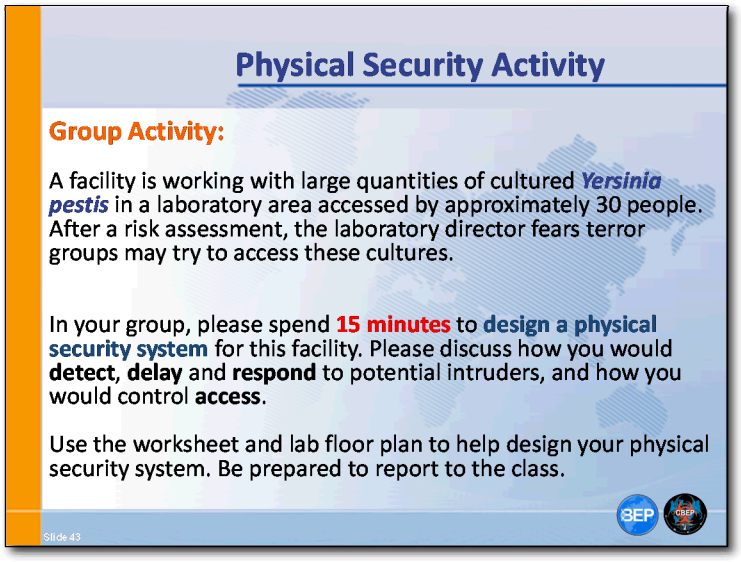
This slide is used to review the expected responses from the previous activity.

Ask: Any questions about Physical Security Performance?

Transition to Case Study

Case Study

Slide 43



Case Study

Small group activity (30 minutes).

Activity Instructions (to students)

1. In your group, please spend 15 minutes to review the scenario and design a physical security system for the facility.
2. Also discuss how you would detect, delay and respond to potential intruders, and how you would control access.
3. Use the worksheet and lab floor plan to help design your physical security system and be prepared to report to the class.

You have 20 minutes to complete this activity

Directions for Instructor:

- After 15 minutes, ask the students to stop working on the exercise
- Lead a 10-minute plenary discussion. Begin by asking for one group of students to report their physical security system and have the students elaborate on specific components.
- Be sure to highlight any similarities, differences or unique answers.
- Note: alternatively, you could assign certain components of the physical security system to different groups and come up with a combined plan for the whole class.

Case Study

Expected Responses

General responses should include all aspects covered in the slides under each category. It will be important to make sure that the students begin their mitigation strategy with a risk assessment or a more formalized scenario that they are protecting against. This will help the students to understand that there may be some limitations to the physical security system depending on which scenario they choose, and also have them realize that they cannot reasonably protect against everything.

Students should include a focus on agent properties and characteristics when designing their physical security system. These are all factors that should be included in the initial risk assessment, such as:

- Pathogenicity – ability to cause disease
- Virulence – degree of pathogenicity
- Host range – restricted tor broad, human, animals, plants
- Communicability – are there reports of epidemics?
- Transmission – means (e.g., direct contact, vector borne) and routes (e.g., ingestion, inhalation)
- Environmental Stability
- Ease of making into a bioweapon

New Responses from Students:

Review

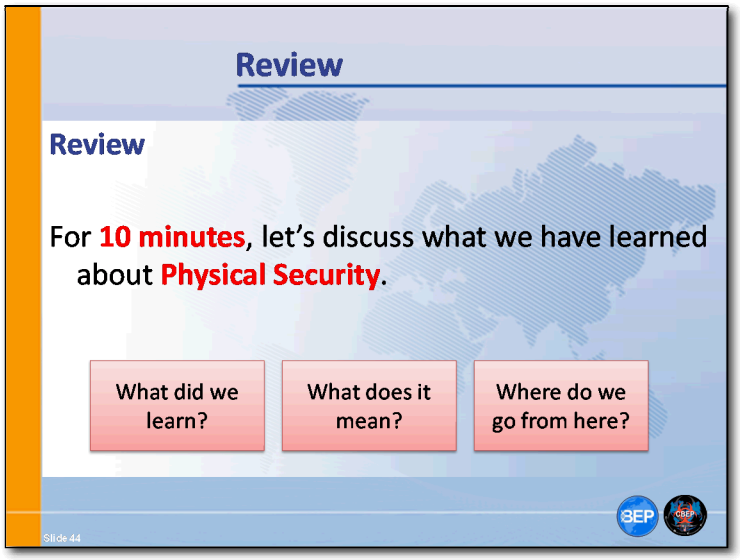
Goal

The purpose and goal of this section is to recap the key messages of the course and to conduct a “What? So What? Now What?” review of the course and key messages.

Time

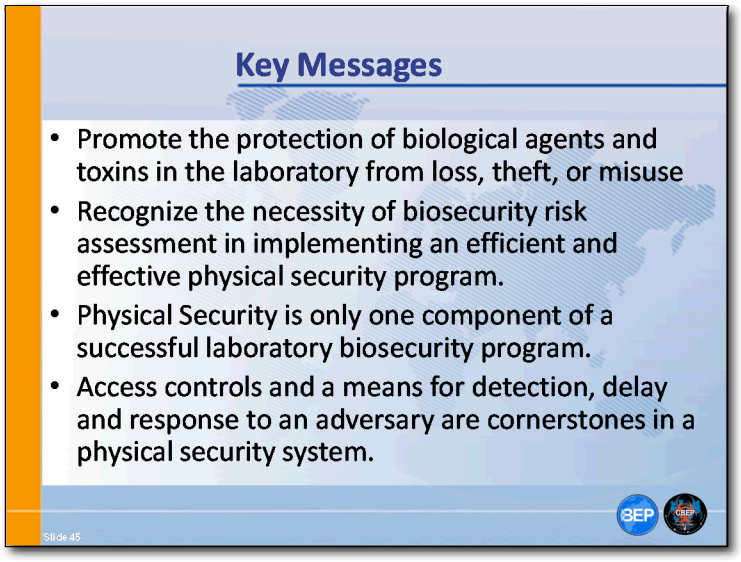
Allow 20 minutes to get through the Review section.

Slide 44



Review

Slide 45

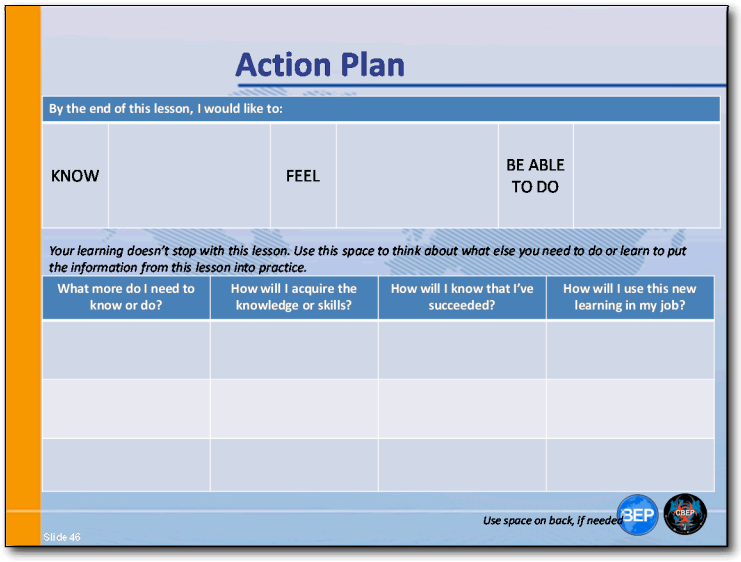


Review Key Messages

1. Promote the protection of biological agents and toxins in the laboratory from loss, theft, or misuse
2. Recognize the necessity of biosecurity risk assessment in implementing an efficient and effective physical security program.
3. Physical Security is only one component of a successful laboratory biosecurity program.
4. Access controls and a means for detection, delay and response to an adversary are cornerstones in a physical security system.

Review

Slide 46



Ask students to spend a few minutes reviewing and completing their action plan.

Slide 47

Review

Level 1 Evaluation

- Ask students to complete the course evaluation and to put it in the evaluation box (alternately, give students instructions for completing the evaluation on-line).