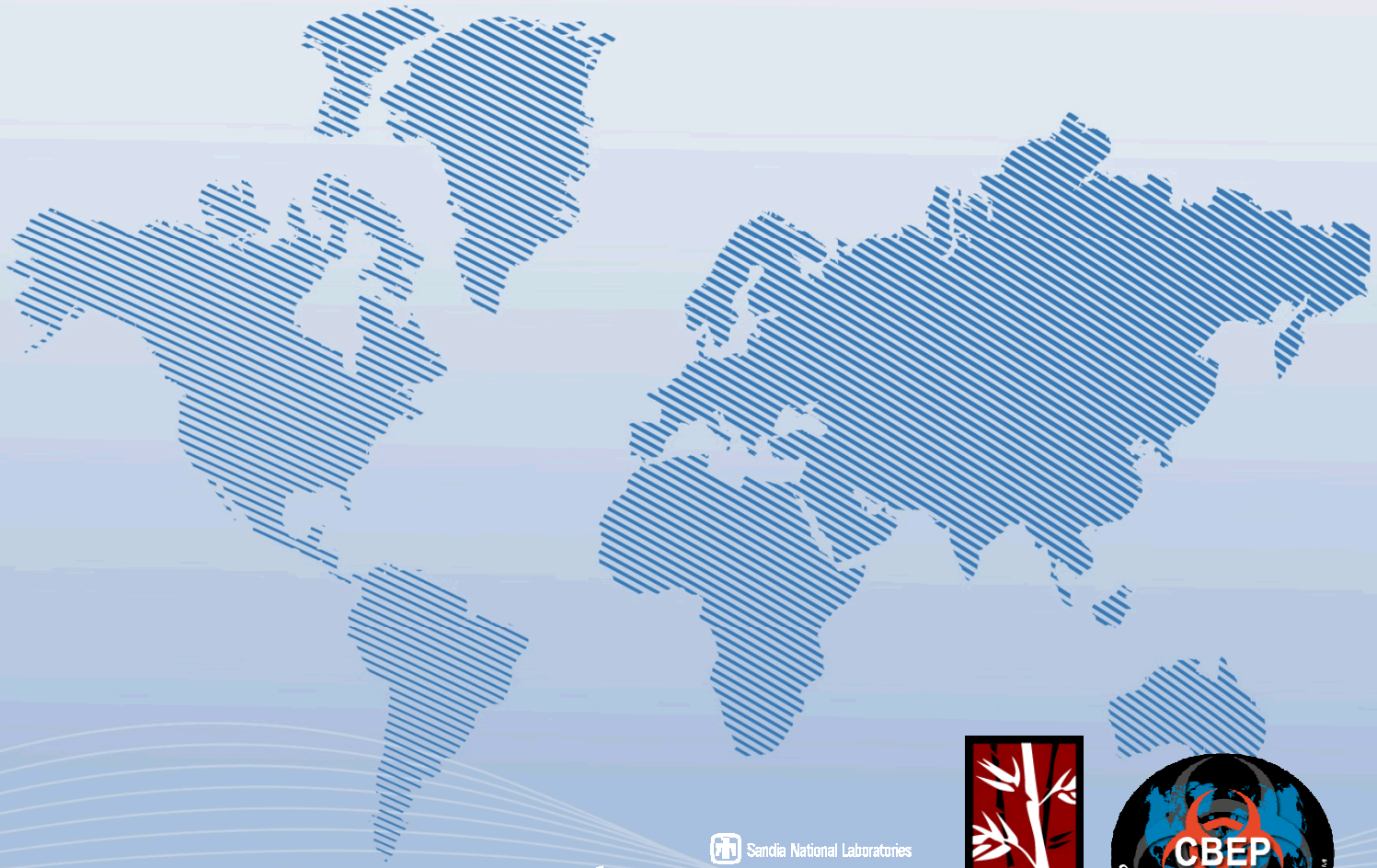
SAND2014-1322P

Laboratory Biosecurity

Instructor Guide



Sandia National Laboratories
International
BIOLOGICAL THREAT REDUCTION

BIOSECURITY ENGAGEMENT PROGRAM

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

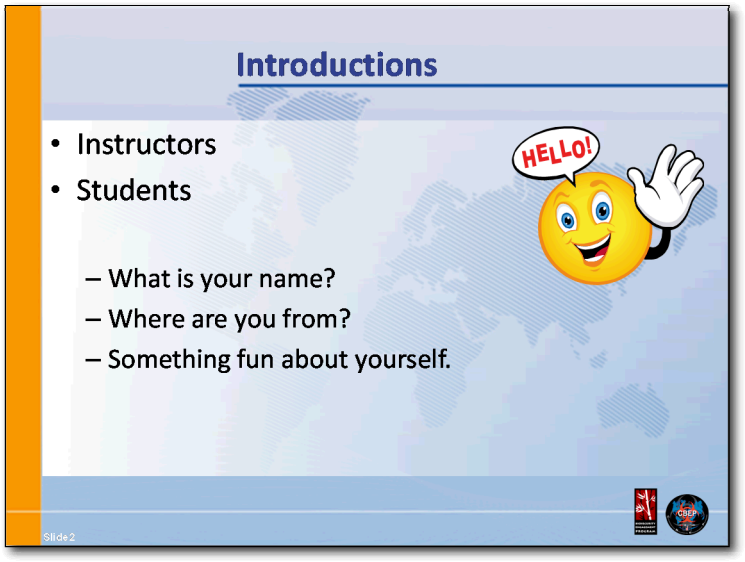
Relevancy of the Course to your experience

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

Welcome & Introductions

Key Messages for Instructor

1. To learn how to protect biological agents and toxins in the laboratory from loss, theft, or misuse.

2. A proper biosecurity risk assessment is necessary before implementing an efficient and effective biosecurity program.

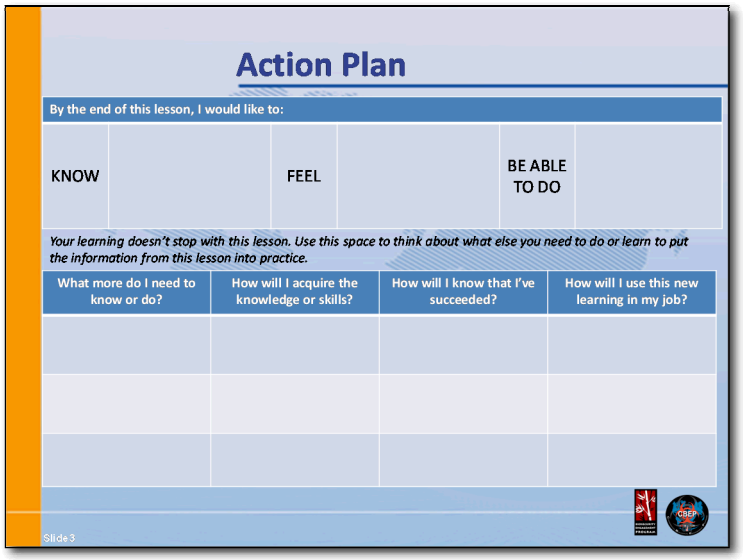
3. Securing pathogens and toxins can be very different from securing other kinds of materials.

4. Physical Security is only one component of a successful laboratory biosecurity program.

5. Material Control and Accountability, Transport Security, and Information Security complement other security components.

6. Security awareness is crucial in laboratory biosecurity.

Slide 3

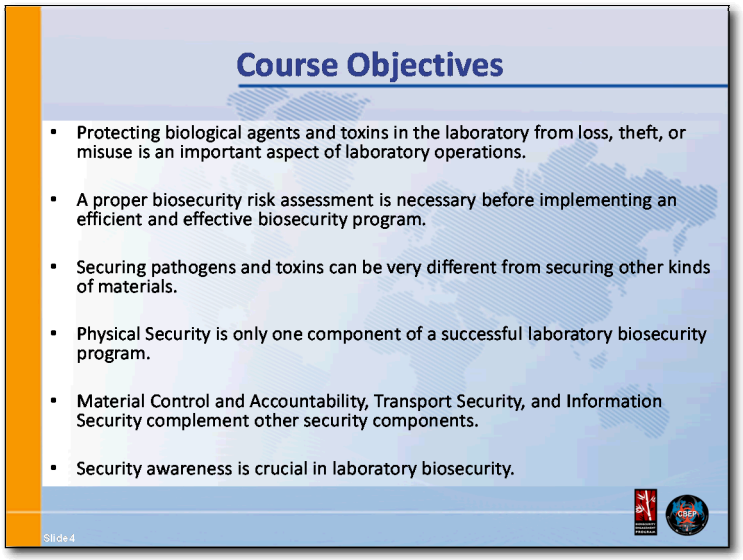


Welcome & Introductions

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

Slide 4



Welcome & Introductions

Background Information for Instructor

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

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

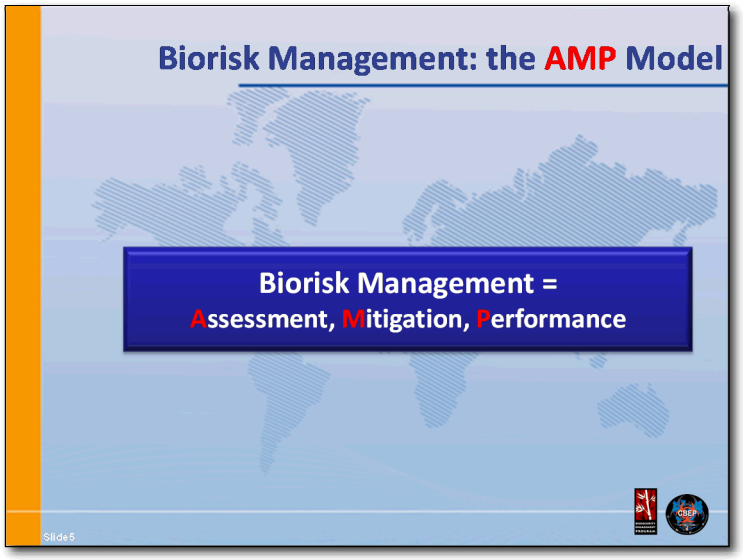
Capture any learning goals that will supplement course objectives and address any that are outside the scope of the course.

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.

Transition to Biorisk Management Touchstone

Biorisk Management

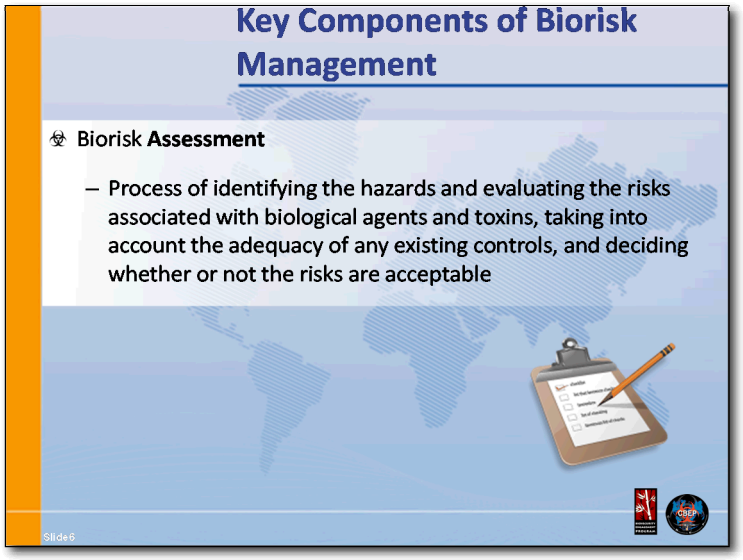
Slide 5



Background Information for Instructor

- Review the AMP model of Biorisk Management with the participants.
- The following three slides provide specific definitions for A, M, and P.
- Integration of laboratory biosafety (protect people from pathogens) and laboratory biosecurity (protect pathogens from people)

Slide 6



Background Information for Instructor

The instructor uses the following three slides: Biorisk Assessment; Biorisk Mitigation; and Performance to define key components of biorisk management

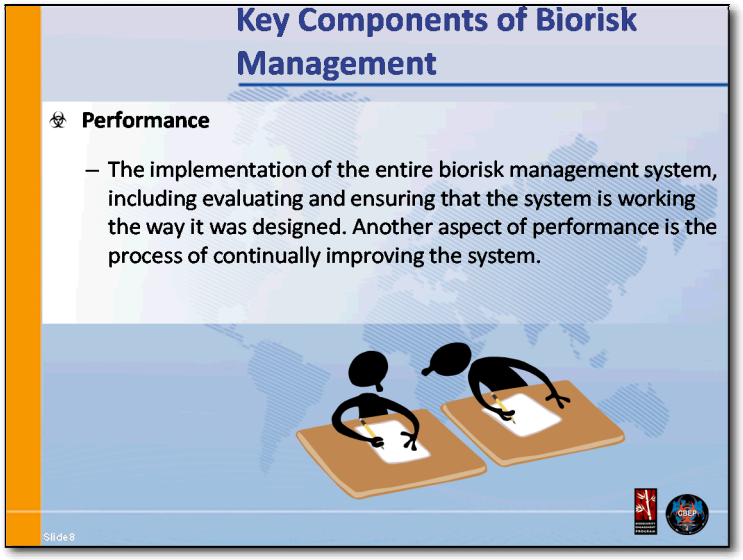
Slide 7

Biorisk Management

Background Information for Instructor

The instructor uses this slide and following slide (Performance) to define key components of biorisk management

Slide 8



Lecture

Taken together, the three elements of AMP constitute a complete biorisk management system.

Take a Break (10 minutes)

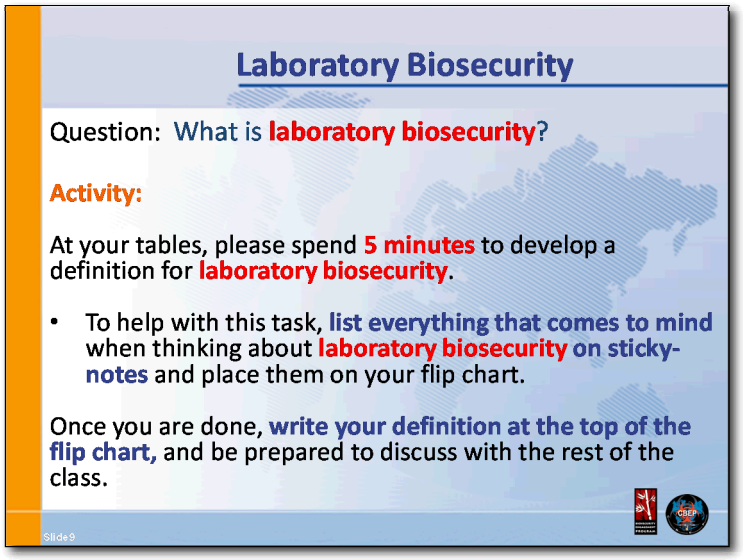
Time Check

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

Transition to Laboratory Biosecurity

Laboratory Biosecurity

Slide 9



Background Information for Instructor

This exercise is designed to introduce the term “biosecurity”. We would like the students to develop a definition for biosecurity from which the rest of the course will be built upon.

Small group activity (10 minutes).

Activity Instructions (to students)

- You have 5 minutes, in your groups, to develop a definition for laboratory biosecurity.
- To help with this task, list everything that comes to mind when thinking about laboratory biosecurity on sticky-notes and place them on your flip chart.
- Be prepared to report your definition and rationale to the class.

Laboratory Biosecurity

You have 15 minutes to complete this activity

Directions for Instructor:

- After 5 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 definition and what they came up with during their laboratory biosecurity brainstorm session.
- Continue around the room, asking other groups to report out, as time allows.
- Be sure to highlight any similarities, differences or unique answers.

Laboratory Biosecurity

Expected Responses

Laboratory Biosecurity Definition

A set of preventive measures designed to reduce the risk of intentional removal (theft), release, or misuse of valuable biological material in order to cause harm to others.

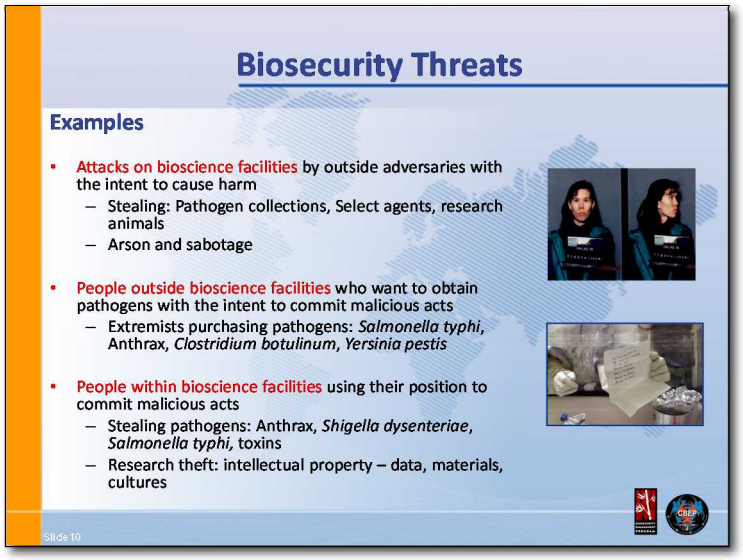
Laboratory Biosecurity Brainstorm

- Theft
- Misuse
- Intentional exposure
- Physical security
- Material security
- Information security
- Deliberate attacks
- bioterrorism
- Select agents

New Responses from Students:

Laboratory Biosecurity

Slide 10



Background Information for Instructor

Now that a formal definition of laboratory biosecurity has been presented, spend a couple of minutes detailing and illustrating examples of biosecurity threats.

The following section highlights specific details about the incidents listed in the slide. As time allows mention the background info.

Laboratory Biosecurity

Background Information for Instructor

<u>Attacks on bioscience facilities by outside adversaries with the intent to cause harm</u>

Stealing -

- An attempt to steal pathogen collection from the central reference laboratory for animal health in Indonesia.

Arson and sabotage -

- 1987: Animal Liberation Front arson attack on UC Davis Animal Diagnostics Laboratory, Damages: $5.1 million, 1 building and 20 vehicles destroyed
- 1989: ALF sabotage of Texas Tech University, Damages: $700,000, destroyed records and computers
- 2002: ELF arson of University of Minnesota's Microbial and Plant Genomics Research Center while building was under construction, Damages: $250,000

Theft of animals -

- 1987: Band of Mercy theft of infected cats from Beltsville Agricultural Research Center
- 2005: ALF stole 10 – 21 mice and vandalized lab at Louisiana State University School of Veterinary Medicine

Laboratory Biosecurity

Background Information for Instructor

People outside bioscience facilities who want to obtain pathogens with the intent to commit malicious acts

Extremists purchasing pathogens –

- 1984 Rajneeshee religious cult attacks, The Dalles, Oregon. Wanted to gain control of the Wasco County Court by affecting the election. Used **Salmonella typhimurium**, purchased from commercial supplier and disseminated in restaurant salad bars. Resulted in at least 751 illnesses, Early investigation by CDC suggested the event was a naturally occurring outbreak. Cult member arrested on unrelated charge confessed involvement with the event
- 1990s Aum Shinrikyo attempts in Tokyo, Japan with the objective to Fulfill apocalyptic prophecy. Used **Bacillus anthracis** (Vaccine strain), **Clostridium botulinum** (Environmental isolate, Avirulent strain) Aum Shinrikyo ordered *Clostridium botulinum* from a pharmaceutical company. Dissemination: Aerosolization in Tokyo (B. anthracis and Botulinum toxin) Leader Asahara was convicted of criminal activity
- 1995—Larry Wayne Harris, a white supremacist, ordered 3 vials of **Yersinia pestis** from the ATCC

Laboratory Biosecurity

Background Information for Instructor

<u>People within bioscience facilities using their position to commit malicious acts</u>

Stealing pathogens: -

- 1995—Laboratory technician Diane Thompson removed **Shigella dysenteriae** Type 2 from hospital's collection and infected co-workers
- 2003 - Professor Thomas Butler, United States, 30 vials of **Yersinia pestis** missing from lab (never recovered, apparently use in a field trial at University of Tanzania that addressed the question of which antimicrobials were effective against Y. pestis in umans that caught the plague ; Soviets onlyones to weaponize); Butler served 19 months in jail.
- Dr. Mario Jascalevich, New Jersey doctor, accused of poisoning 5 patients with this plant-derived toxin - **Tubocurarine**: 1966
- Japan 1964-1966, Dr. Mitsuru Suzuki was a physician with training in bacteriology and wanted revenge due to deep antagonism to what he perceived as a prevailing seniority system. He used **Shigella dysenteriae** and **Salmonella typhi** to disseminate via Sponge cake, other food sources. He was later implicated in 200 – 400 illnesses and 4 deaths. The Official investigation started after anonymous tip to Ministry of Health and Welfare. He was charged, but was not convicted of any deaths.

Research theft -

- Two former post-docs at Harvard Medical School indicted by grand jury for theft of research materials. They shipped 20 boxes of materials related to drug discovery research to new employer in Texas.

- Post-doc at Cornell arrested with >250 test tubes, vials, and petri dishes in luggage before boarding a flight to Shanghai

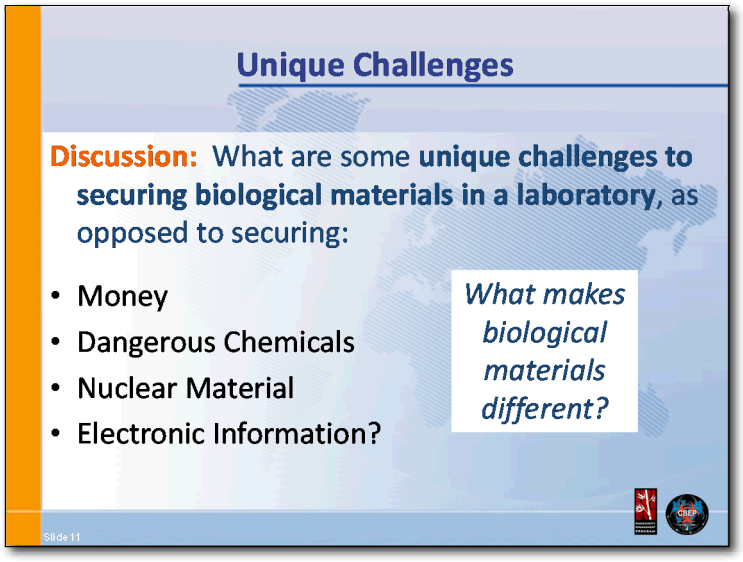
Laboratory Biosecurity

Ask: Any questions on introduction to Laboratory Biosecurity?

Transition to Unique Challenges

Unique Challenges

Slide 11



Plenary discussion

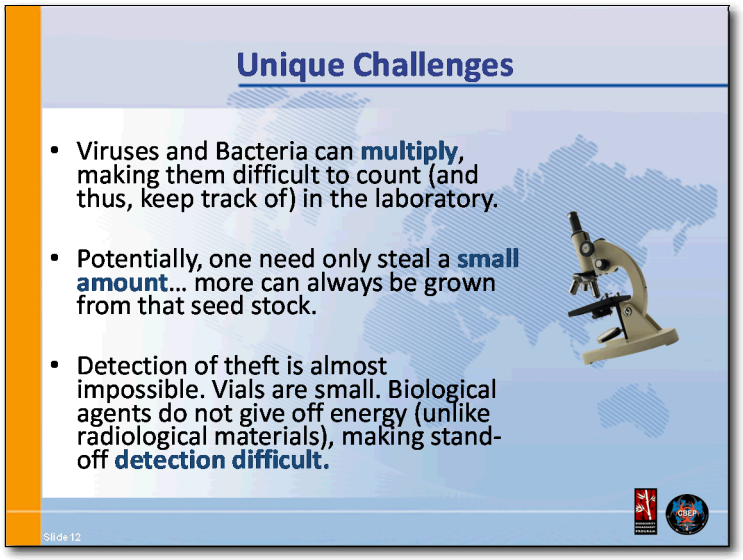
Unique Challenges

Lecture

- Designing and implementing a cost-effective laboratory biosecurity system depends, first and foremost, on recognizing the unique nature of biological assets.
- Traditional security approaches applied to very high-value items or unique dangerous materials, such as special nuclear materials, may not directly translate to the operating reality of the bioscience institution. Laboratories may (or may not) be actively using/moving materials as part of their missions, so biosecurity design has to accommodate mission requirements. For instance, importance should be placed on securing the biological asset in its current location instead of bunkering it in a single location where it can be stored long term. For this reason, traditional probability and risk assessment tools to not work within biosecurity.
- With few exceptions, biological agents occur naturally. Dangerous pathogens and toxins are also worked with at hundreds of legitimate bioscience laboratories around the world.
- It is important for security designers to understand that a legitimate bioscience institution's possession of a dangerous biological agent does not imply malicious intent.
- All dangerous biological materials are known as fundamentally "dual-use" materials: they have legitimate defensive and peaceful commercial, medical, and research applications but they could also be misused to intentionally cause infectious disease.

Unique Challenges

Slide 12



Lecture

- Pathogens are self-replicating organisms, making the theft of any amount potentially significant for a bioterrorist.
    - The notion of self-replication, as well as unpredictable mutation and death, also prohibits the reliable quantitative accounting of biological agents through their lifecycle.
- Also, in contrast to nuclear materials or chemicals, biological agents emit so little energy that they are not detectable with "stand-off detectors," making it virtually impossible for a security system to identify someone illicitly removing biological materials from a facility.

Unique Challenges

Slide 13

Unique Challenges

In plenary, ask students:

Where can you find biological materials in the laboratory?

Expected Response:

- At a bioscience institution, these biological agents can be found in many different physical locations in many different forms.
    - For example, biological agents exist in freezers, incubators, animals, carcasses, animal bedding, and waste material – pretty much everywhere.

What should we protect?

Have the students consider the questions on the slide to think about what in the laboratory may need protection

Expected Response:

- This will depend on the laboratories risk assessment. These factors should be taken into consideration during the risk assessment.

How should we protect?

Now that the students have thought about where the biological material is and what to protect, have them think about how this could be achieved. Prompting questions:

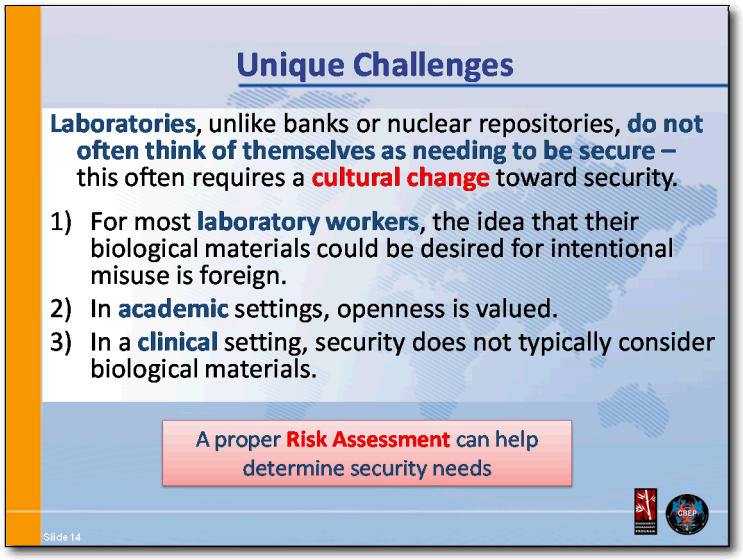
- How do we secure something that is everywhere?
- Where do we draw the boundaries? And How do we justify those boundaries?

Expected Response:

- Locks, access controls, passwords
- It is hard to secure something that is everywhere
- It is important to maintain security of the pathogen in whatever physical location it is in, rather than bunkering a single location where it is stored long term. Note: This decentralization makes restricting access to authorized individuals extremely difficult.

Unique Challenges

Slide 14



Lecture

Often, because laboratories don't often think of themselves as needing to be secure, they are vulnerable to theft and other biological misuse.

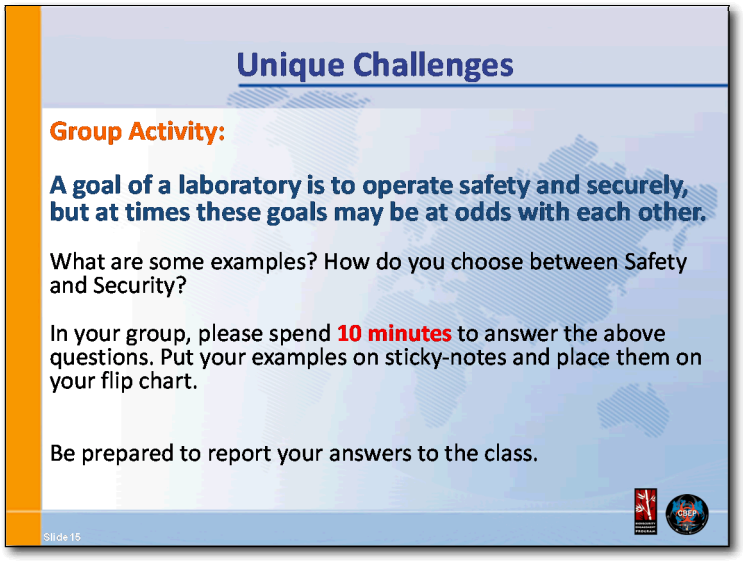
The cultural shift toward security can be difficult for laboratory personnel. Biologists sometimes feel hindered or don't understand security systems that are dominated by traditional means, which was not designed with any recognition of the unique attributes of biological materials.

Bioscience laboratory personnel and management have a similar responsibility to implement biosecurity systems, but the concepts of biosecurity are much less understood than biosafety.

Management and laboratory personnel must understand why biosecurity is important and work toward achieving a secure working environment in a variety of settings.

Unique Challenges

Slide 15



Unique Challenges

Small group activity (20 minutes).

Activity Instructions (to students)

1. A goal of a laboratory is to operate safety and securely, but at times these goals may be at odds with each other. – REMIND STUDENTS OF DIFFERENCE BETWEEN "BIOSAFETY" AND "BIOSECURITY"
2. What are some examples? How do you choose between Safety and Security?
3. In your group, please spend 10 minutes to answer the above questions. Put your examples on sticky-notes and place them on your flip chart.
4. Be prepared to report your answers to the class.

You have 15 minutes to complete this activity

Directions for Instructor:

- After 15 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 information examples and have the students elaborate on what factors they considered.
- Continue around the room, asking other groups to report out, as time allows.
- Be sure to highlight any similarities, differences or unique answers.

Unique Challenges

Expected Responses

What are some examples?

Signage: Biosafety want to advertise the fact that dangerous agents are present to safely identify hazardous substances and responsible parties, whereas, biosecurity wants to avoid identifying potential target materials or access to those materials.

Exits: Biosafety promotes easy exit in case of an incident, while biosecurity inherently has containment and limited egression on the agenda, e.g. the case of theft etc.

Emergency response: Biosafety supports providing emergency responders with locations of hazards, the identities of responsible individuals, and access to the laboratory, whereas biosecurity strives to control the distribution of sensitive information only to those with a need to know rationale. It also works to prevent people from moving into or through restricted areas.

Inventory accessibility

How do you choose between safety and security?

A Risk Assessment

Laws, regulations, building codes

New Responses from Students:

Unique Challenges

Slide 16

Background Information for Instructor

This slide wraps up the major points from the unique challenges section. It is important to note that in addition to these considerations, communication about potential risks is an important aspect of a biosecurity program.

Risk communication is an interactive process of exchange of information and opinion on risk among risk assessors, risk managers, and other interested parties.

Ask: Any questions about Unique Challenges?

Take a Break (10 minutes)

Unique Challenges

Time Check

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

Transition to Physical Security

Physical Security

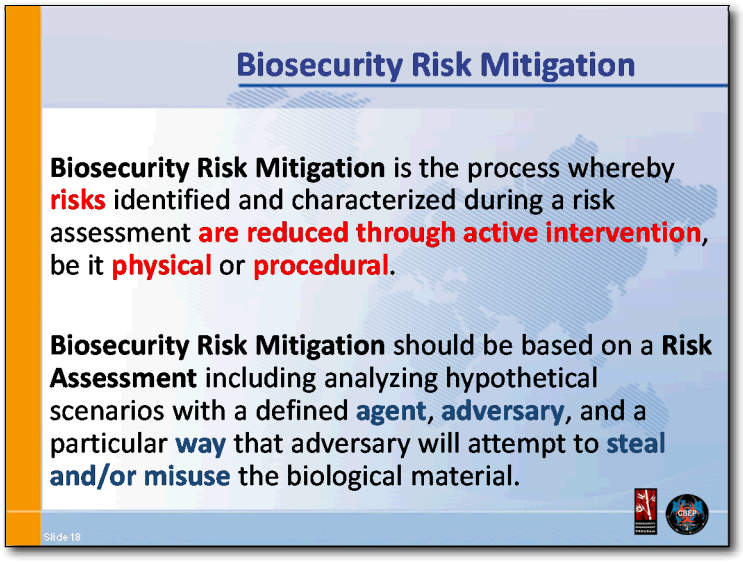
Slide 17

Background Information for Instructor

This slide introduces the remainder of the course, which will be focused on Laboratory Biosecurity Risk Mitigation, in the context of the AMP model.

Physical Security

Slide 18



Physical Security

Background Information for Instructor

In addition to a risk assessment, it is useful to use scenarios in which a defined agent, adversary etc., are considered to to detect any vulnerability in the biosecurity management program. This is also known as a Design Basis Threat (DBT), which is the defined threat, which a security system is supposed to protect against.

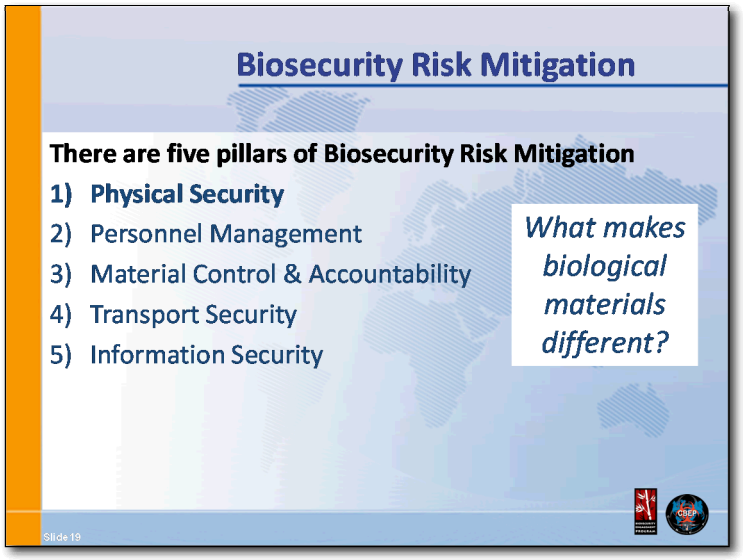
Laboratory biosecurity risk mitigation measures should be more robust for higher risk scenarios than for lower risk scenarios.

Useful questions that should be included in the risk assessment may include:

- What things of value—or assets—will the biosecurity system protect?
- What threats will the biosecurity system protect those assets against?
    - In general, the more assets a security system must protect, and the more threats the security system must protect those assets against, the more intrusive the security system will be to the facility's operations and the more expensive it will be to install and maintain.

Physical Security

Slide 19



Background Information for Instructor

A comprehensive biosecurity program includes a combination of each of these components, which make up the five pillars of biosecurity risk mitigation. These components make up the focus points of the biorisk management program and implementation of each of these elements will be based on each facility's unique risks. We will discuss each of these components in more depth.

Physical Security

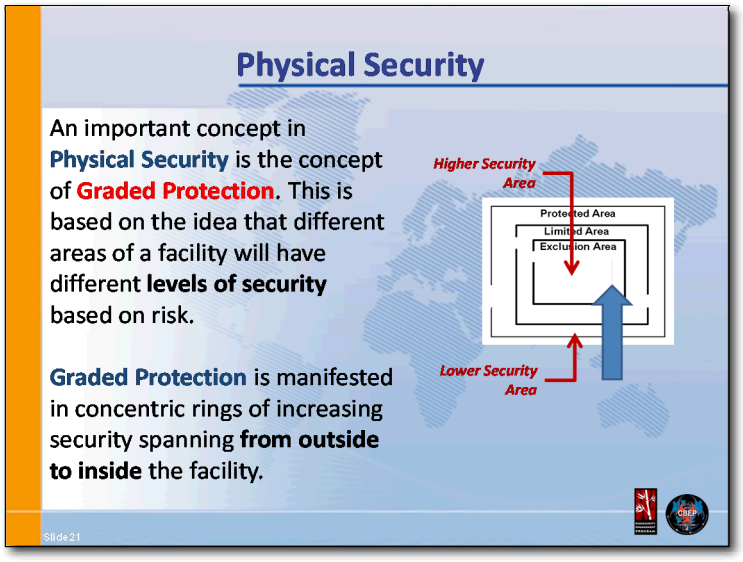
Slide 20

Background Information for Instructor

Physical security is often the most obvious way to reduce risk against an outside threat/adversary. Physical security seeks to reduce the risk of unauthorized access to specific areas or assets. This type of security is often accomplished with a mix of several fundamental elements, including security barriers, access controls, intrusion detection mechanisms and also means for alarm assessment. Taken together these means will be work to detecting, delay and respond to an intrusion.

Physical Security

Slide 21



Physical Security

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.

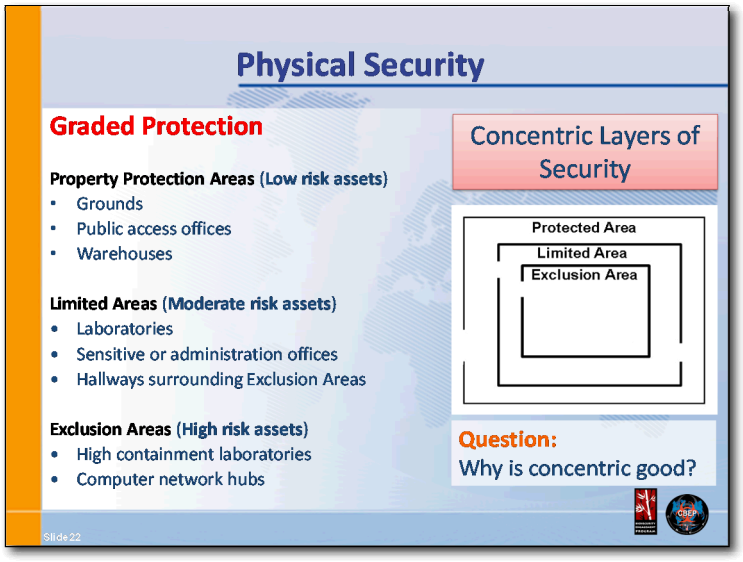
Keep in mind that the overall layout of the facility and the locations of access control features to access the inner layers of the physical security system are important to consider in order to ensure that the normal and emergency paths of employees and visitors do not inadvertently leave gaps in security 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

Slide 22



Physical Security

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.

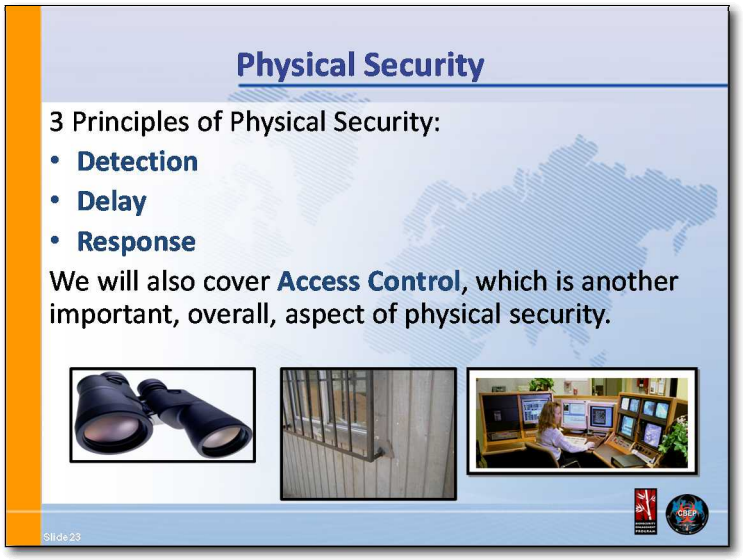
The nested levels of protection are referred to as “Property Protection Areas,” “Limited Areas,” “Exclusion Areas,” and “Special Exclusion Areas.” Limited, Exclusion, and Special Exclusion Areas are always considered to be restricted areas as the term is used in the preceding sections.

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

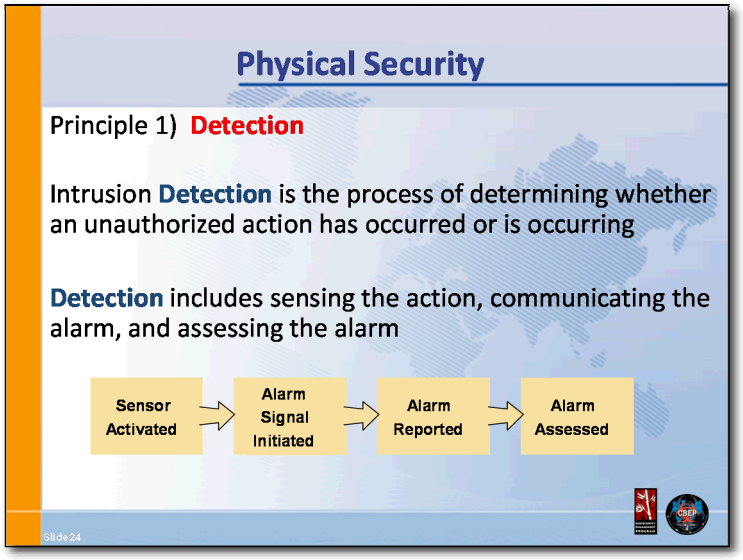
Slide 23



Lecture

These are the 3 areas that we will focus on in our discussion of physical security. Another important topic that spans all three of these principals is that of Access Control.

Slide 24



Physical Security

Background Information for Instructor

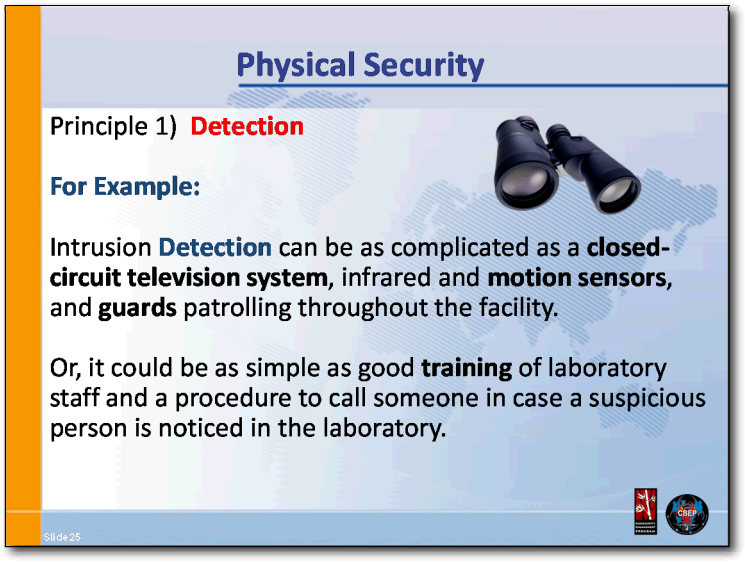
Intrusion detection systems alert security personnel to attempts to gain access without authorization. The detection aspect of physical security has many components that allow the process to work as a whole. In this context, detection includes sensor activation, the alarm signal initiation, the alarm is assessed to determine the nature of that change in status, then the alarm is reported

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 nuisance 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.

Physical Security

Slide 25



Physical Security

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

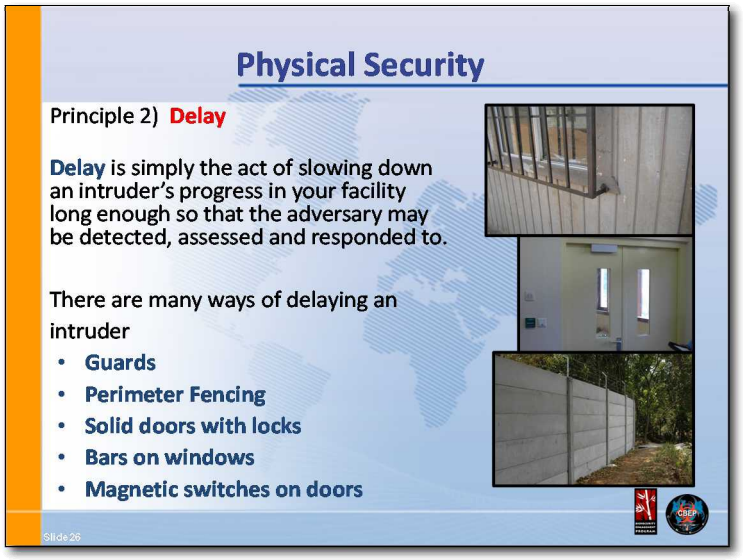
- Motion sensors, cameras (with adequate lighting), seals, strong door, no windows, guard patrols, electronic intrusion detection systems (with constant monitoring)
- If forced entry occurs, or if a door or other monitored entryway is open for an extended period of time, an alarm will be generated.
- Intrusion detection sensors/the electronic network can be configured to detect tampering so that if a communication line is cut or a junction box (or sensor) 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.
- Potential access points, ie 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 types 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.

Physical Security

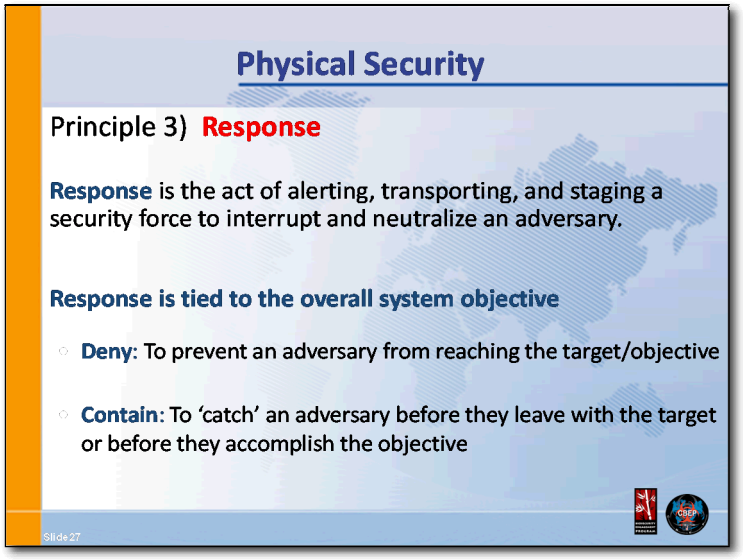
Slide 26



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.

Slide 27



Physical Security

Background Information for Instructor

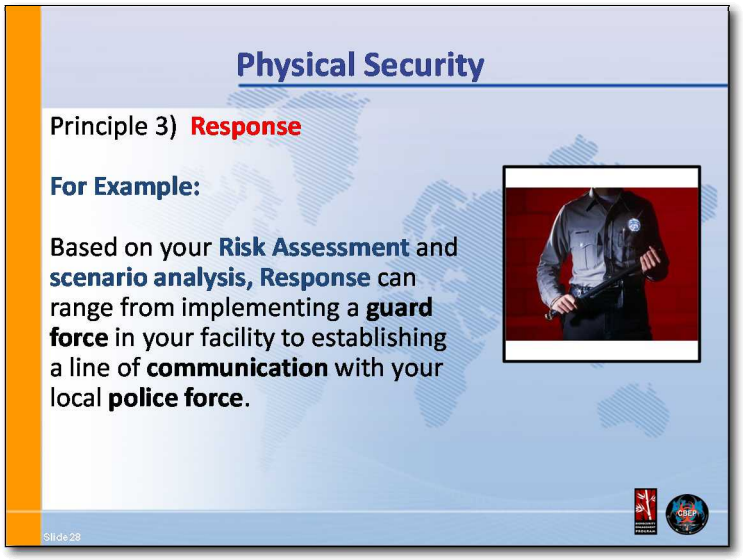
If the alarm sounds and the threat is assessed to be valid, a response to the situation must be made to try to apprehend the intruder. A response may come from a security guard force or a call may be made to the police. Only authorized personnel should try to handle an encounter with an intruder. Unauthorized 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.

Physical Security

Slide 28

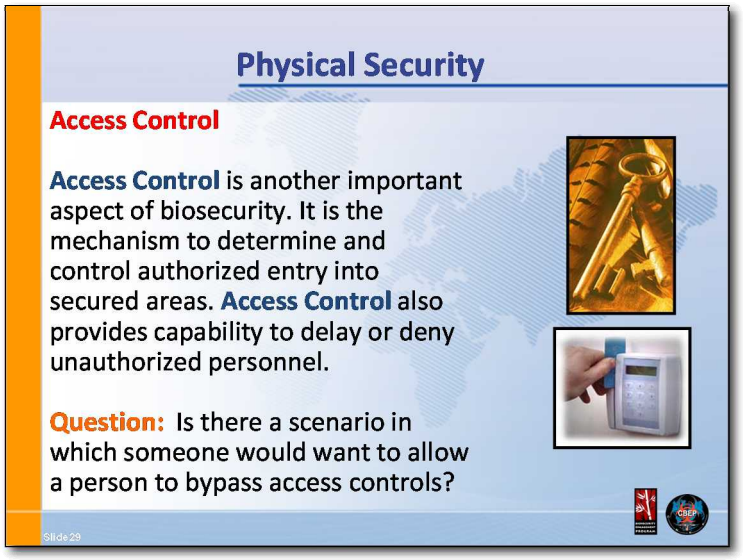


Background Information for Instructor

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.

Physical Security

Slide 29



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.

Physical Security

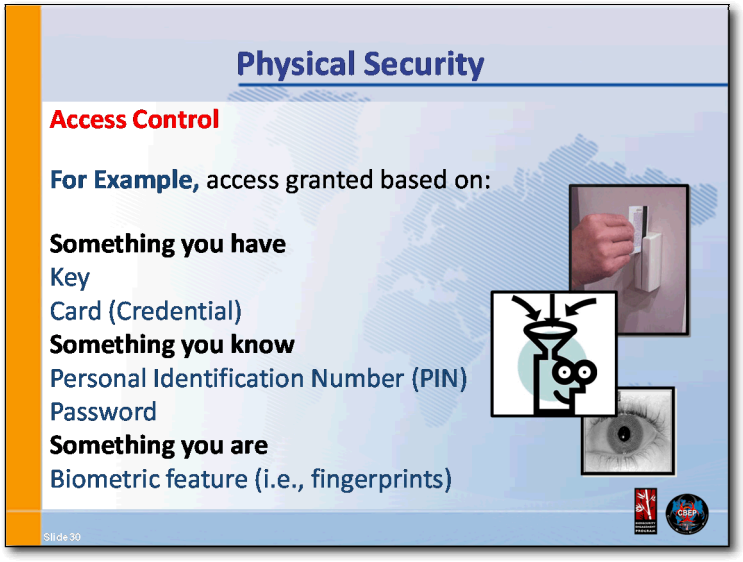
In plenary, ask students:

Is there a scenario in which someone would want to allow a person to bypass access controls?

Expected Response:

The answer to this question can vary. The main point should be that access controls should NOT be bypassed without a really good, documented, reason. An example may include emergency personnel or for maintenance. In any case, strict policies and procedures should also be in place along with access controls to make sure they are effective, and these should address any instances where the access control system may be authorized for bypass.

Slide 30



Physical Security

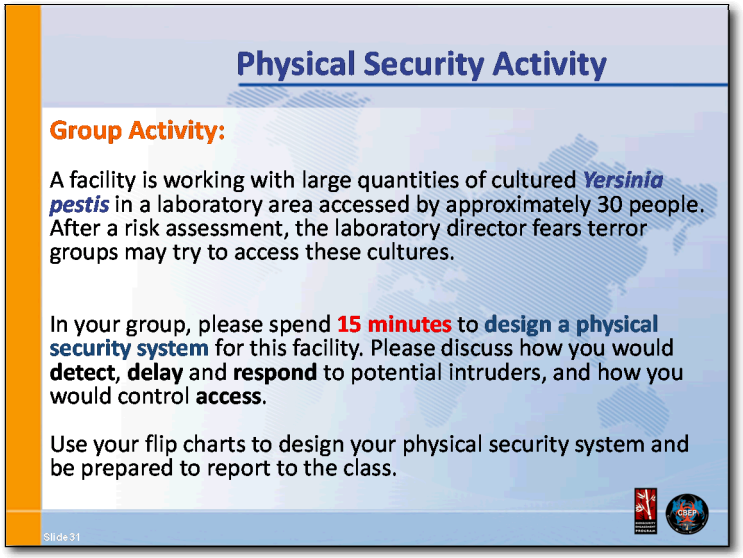
Background Information for Instructor

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.

Slide 31



Physical Security

Small group activity (20 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 your flip-charts to 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 5-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.

Physical Security

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.

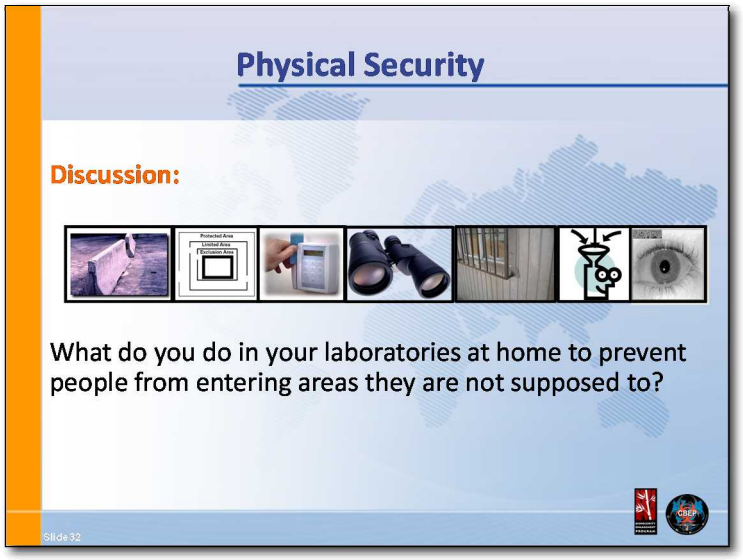
Students should include a focus on agent properties and characteristics when designing their physical security system. These are all factors that should be included in the initial risk assessment, such as:

- 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:

Physical Security

Slide 32



Ask students to REFLECT individually on the following question/statement:

What do you do in your laboratories at home to prevent people from entering areas they are not supposed to?

Ask: Any questions on Physical Security?

Take a Break (10 minutes)

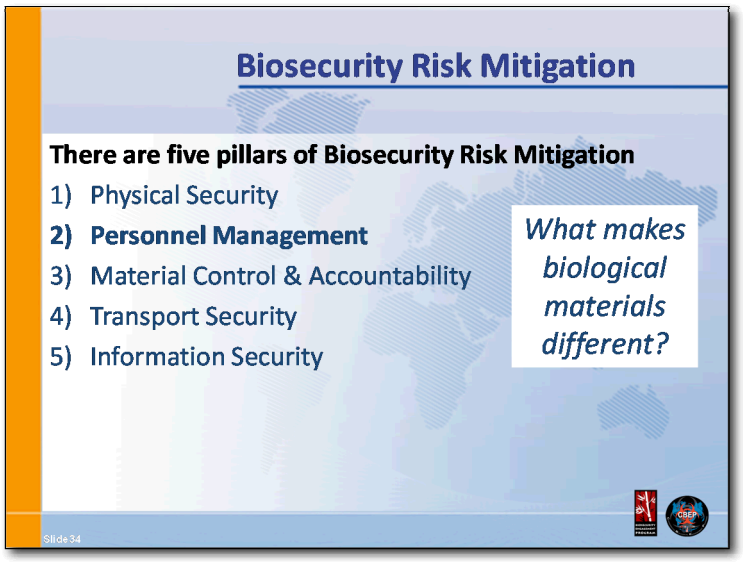
Time Check

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

Transition to Personnel Management

Personnel Management

Slide 33

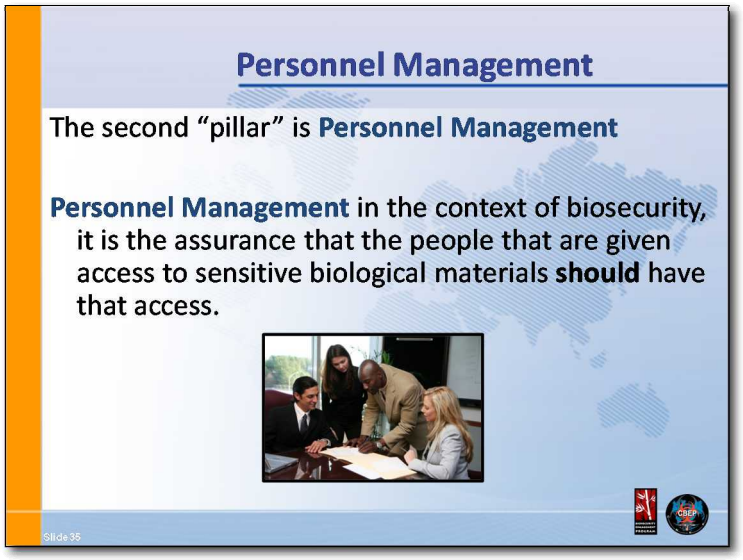


Lecture

A comprehensive biosecurity program must include a combination of all the pillars of Biosecurity Risk Mitigation. Now we will focus on the Personnel Management component.

Personnel Management

Slide 34



Background Information for Instructor

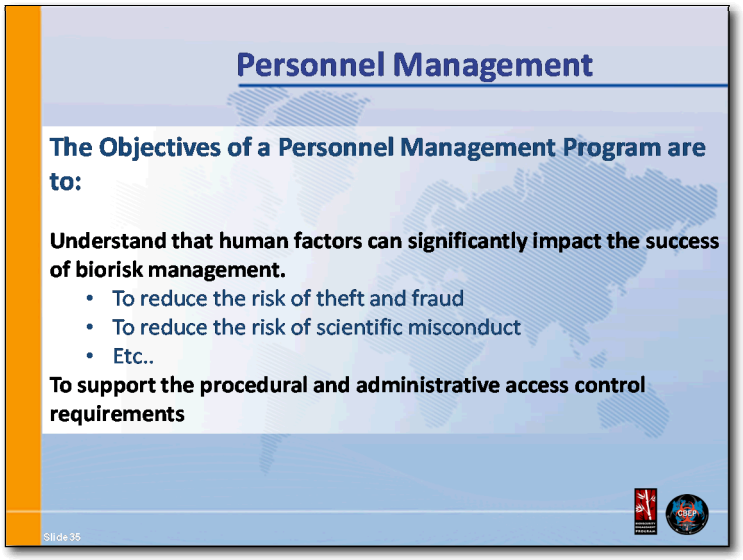
Personnel management is the principal security measure for addressing threat from personnel that are already associated with the laboratory. It is fundamentally about ensuring that only trusted individuals are given authorized access to restricted areas.

The principal objective of personnel security programs and personnel management programs in bioscience institutes is to protect members of the scientific, public health, veterinary, and medical communities.

This information is designed for those who are working at the laboratory level. While much of human performance management is left to the leaders and managers, it is important for all workers to be familiar with basic principles of human performance and how these may impact the safety and security of biological material.

Personnel Management

Slide 35



Background Information for Instructor

A personnel management program relies on the understanding that human factors can significantly impact the success of biorisk management overall. For example, the effectiveness of any security system, no matter how technologically advanced, is ultimately determined by the training, reliability and integrity of the individuals who operate it. In the larger context, this understanding will help to reduce the risk of theft, fraud and scientific misconduct etc. In a more defined context, personnel management is needed to support the procedural and administrative access control requirements.

Due to the nature of working in a laboratory that includes potential access to agents, materials and equipment that may be used destructively, authorizing access to personnel must be taken very seriously.

The level of impact of personnel management programs for reducing risk is questionable, however, ideally, they would, if implemented properly, serve to protect the integrity of research programs and affiliated personnel. Overall, in a biosecurity framework, a personal management system is part of the overall protective posture, and supplements safety and security measures.

Personnel Management

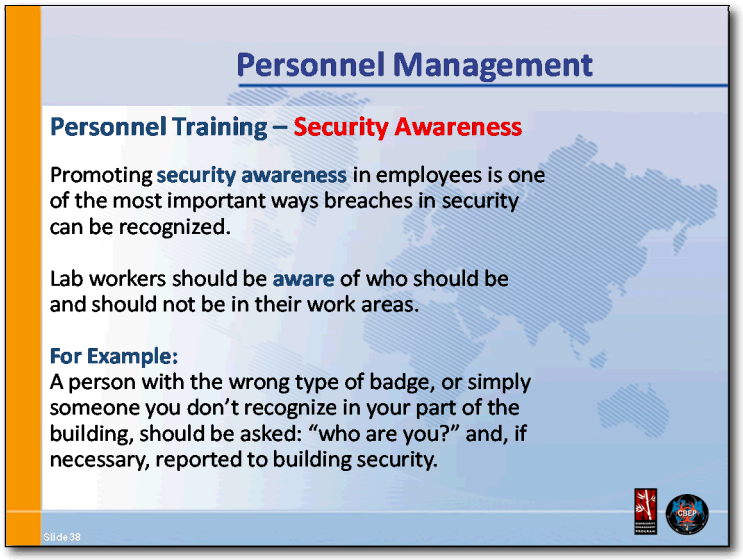
Slide 36

Background Information for Instructor

Human performance depends on several factors, not just on the individual. Aspects of the job including the setting and workplace values as well as organization characteristics like expectations and assessment of progress will also contribute to overall human performance in the workplace. It is human nature to try and make an individual solely responsible for their errors but that is a short-sighted view. Instead, it is important to consider all these factors to maximize the productivity of the people in the workplace. This is the first step in reducing risk originating from personnel actions.

Personnel Management

Slide 37



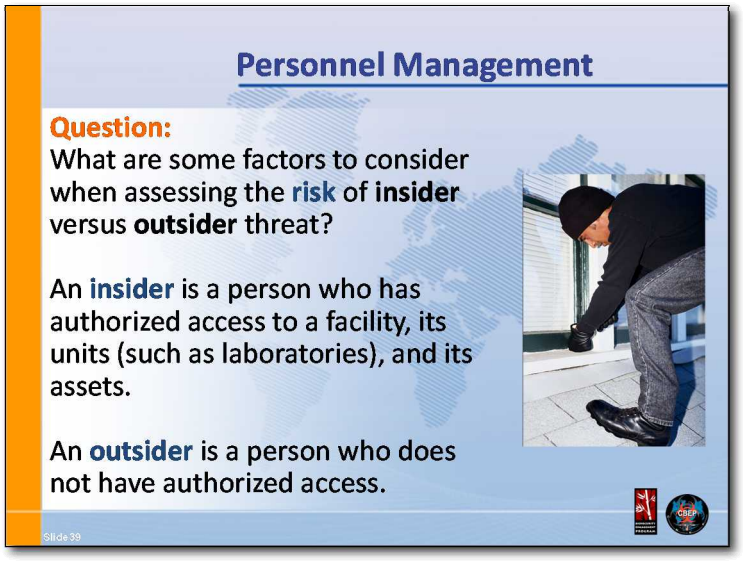
Background Information for Instructor

Another aspect of personnel management includes security awareness, which can help to reduce risk by training personnel to recognize situations where safety or security may be jeopardized. The best example of this is an employee identifying another employee in a restricted area where the second employee does not have access. This security breach can then be reported to appropriate management.

There are different levels of risk associated with threat from an insider (a person who has authorized access to a facility and its assets) compared to an outsider (a person who does not have authorized access). This topic about insiders can often be a tricky subject to broach, because no one wants to think that their colleagues might present a security risk, even though they could. We will analyze these threats in the next activity.

Personnel Management

Slide 38



Personnel Management

In plenary, ask students:

What are some factors to consider when assessing the risk of insider versus outsider threat?

Expected Response:

The purpose of this question is to highlight the fact that motive for biosecurity risk can be very difficult (if not impossible) to discern. This will give the students the opportunity to discern why: we can't get into the minds of other people. Hopefully, this will also push students into considering "opportunity" and "means" as more reliable ways of characterizing adversaries relevant to the facility.

Insiders tend to pose a greater threat than outsiders because they typically have both greater means and opportunity than an outsider. Insiders, however, do not necessarily have different motives than outsiders.

Follow up questions:

Why might the motive of a potential adversary either inside or outside a facility be so difficult to determine?

Are there any areas where an insider and an outsider may intersect?

What are some mitigations efforts that can be used to reduce the risk associated with insiders? Outsiders?

Personnel Management

Slide 39

Ask students to REFLECT individually on the following question/statement:

What do you do in your laboratories at home to promote a secure work environment in terms of human performance and security awareness?

Ask: Any questions on Personnel Management?

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 Material Control & Accountability

Material Control & Accountability

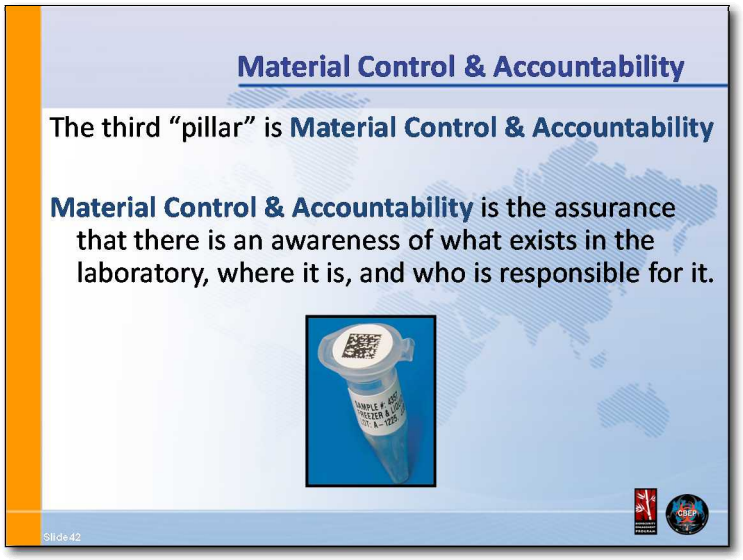
Slide 40

Lecture

A comprehensive biosecurity program must include a combination of all the pillars of Biosecurity Risk Mitigation. Now we will focus on the Material Control & Accountability component.

Material Control & Accountability

Slide 41



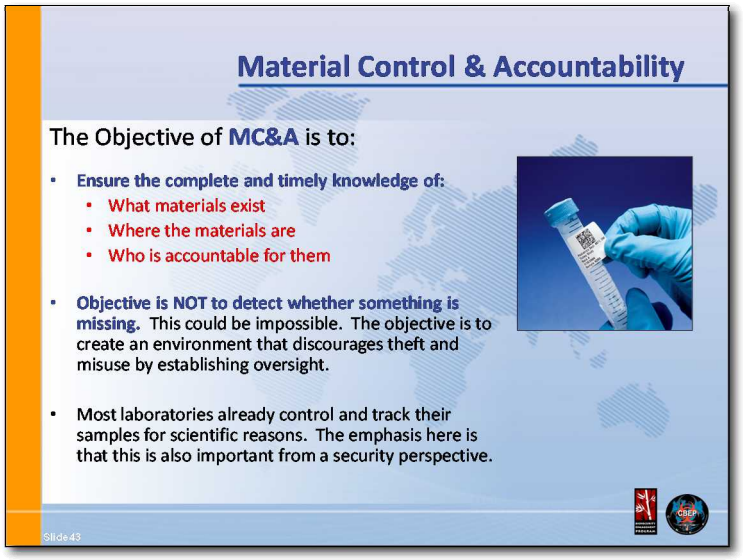
Background Information for Instructor

MC&A seeks to adopt practices that establish and reinforce responsible oversight of work with dangerous pathogens and toxins. MC&A measures help enhance laboratory biosecurity by establishing exactly what biological material is present at a facility, how and where the material is stored and handled, and who is responsible for it.

Control ensures that material is confined to known, legitimate use, while accountability ensures oversight by formally associating material with people and information records.

Material Control & Accountability

Slide 42



Background Information for Instructor

The objective of MC&A measures is to maintain a system of accountability for biological agents. This also creates an environment that discourages insiders from stealing and using biological agents maliciously.

Despite the fact that it is not possible to count every microbe in the laboratory environment, it is possible to take prudent measures to ensure that dangerous pathogens and toxins are controlled in a manner that will, and possibly detect, theft of these materials. At a minimum, MC&A measures can facilitate forensic analysis if an illicit diversion is detected.

MC&A combines policies, procedures, and technologies to augment other elements of laboratory biosecurity during the use, storage, and transfer of material.

Material Control & Accountability

Slide 43

Lecture

There are many important issues that should be taken into consideration when assessing MC&A and how it can be used to reduce risk. To better understand how these issues fit into MC&A we will explore each aspect individually.

Material Control & Accountability

Slide 44

Material Control & Accountability

Background Information for Instructor

The first aspect of MC&A is deciding which materials are subject to control and accountability measures. This can be a complicated process. This decision requires identifying the agents, the form of the agents, and whether quantity is a factor. A thorough risk assessment should identify and categorize those materials that require MC&A measures. Consideration should be given to those subcomponents, any special experimental form, or other variant deemed to present a commensurate risk.

The difficulty in defining "material" subject to MC&A is in the details. Dangerous biological agents can be found in many specimens throughout a typical bioscience institute: repository stock cultures, working stocks, clinical specimens, unknown samples, and genomic material, among other categories.

These specimens are also found in many forms: liquid solution, lyophilized powder, in an infected host, in animal waste, and as contamination on equipment or other objects. Genomic libraries of dangerous pathogens and identified virulence genes from an organism may also be considered material from a MC&A perspective.

It may not be important to include samples of unknown content unless they are suspected of containing dangerous biological agents. Of course, once a sample has been positively identified as a dangerous biological agent, it should be subject to specific MC&A measures that are appropriate to the agent. It must be clear where specific MC&A measures begin and end for specific agents. The manner in which MC&A is implemented may vary for different types and forms of specimens or agents.

MC&A does not apply to equipment, instruments, clothing, and similar laboratory objects that have been, or may have been, contaminated with materials. These items should be decontaminated and, if necessary, disposed of properly in an appropriate area, foregoing the need to include these items in MC&A procedures.

Material Control & Accountability

Slide 45

Lecture

Physical - means of preventing unauthorized access

- Ex. Locking freezer or restricting where research with materials can occur

Administrative-

- Integrated with currently existing, standard laboratory procedures
- Working with material
- Inactivating and disposing of material
- Conducting periodic inventory checks
- Removing material from storage and returning material to storage
- Labeling and tracking

Material Control & Accountability

Background Information for Instructor

Control is implemented to ensure that materials stay where intended and that they are used for a stated purpose by specifically designated and authorized people. Control must deal with all activities involving the material, such as storage, use, transport and disposal.

A complete inventory system is the primary means to establish material control. The following describes the implementation of an inventory system. The physical inventory is assembled by a thorough search and review of all locations where the subject materials may exist. A physical inventory should be conducted periodically, with the frequency depending on the agents involved; the higher the risk, the more frequently physical inventories should be conducted. Whenever a physical inventory is conducted, the results should be compared with the current book inventory, and any discrepancies should be identified. If a discrepancy indicates the possibility of theft, or if the discrepancy remains otherwise unexplained, it should be reported immediately to the accountable individual and, if appropriate, local and national authorities. Conducting a physical inventory includes identifying items, counting items, and occasionally conducting tests to verify contents.

When large numbers of items are involved, especially for lower-risk materials, selective (statistical) sampling for identification or diagnosis may be employed. MC&A information might prove useful to an adversary, so it should be treated as sensitive information and should be subject to information security practices. MC&A information is often intermingled with information recorded for scientific purposes, so care should be taken to prevent sensitive MC&A information from inadvertently being released to the public. A detailed inventory should be kept in a secure, limited-access database. A key aspect of control is to make sure that full audits should be periodically conducted to verify compliance.

Storing and using dangerous biological agents in restricted areas and limiting access to these materials to authorized personnel help establish control. A locked freezer or vault can offer additional control in laboratory spaces that are shared among more individuals than actually work with a particular material. Automated systems can log events such as laboratory access (in and out) or freezer opening and closing, often providing date, time, and personal identification. For example, barcode labels or radio frequency tags are engineered measures that can facilitate inventory.

Material Control & Accountability

Background Information for Instructor

It should be noted that control needs to be effective under both normal conditions and anticipated abnormal conditions wherever possible, such as accidents, power failures, or emergencies. Otherwise, covert diversion of material could be attempted under the cover of an abnormal condition (perhaps intentionally caused).

Slide 46

Material Control & Accountability

Background Information for Instructor

Accountability is the means of ensuring that someone is responsible for the dangerous biological agents stored and/or used within a defined area. Assigning qualified, authorized individuals to oversee the control of protected agents, keeping accurate and timely records, reporting, and auditing are all aspects of accountability.

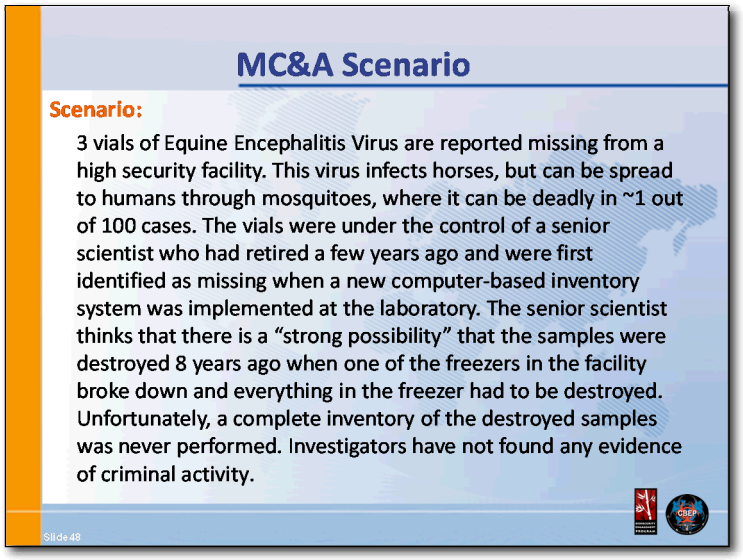
Each dangerous pathogen and toxin should have a designated accountable individual who is knowledgeable about the assigned pathogen or toxin in storage and in use. An "accountable" individual may be assigned on an agent-by-agent basis, on a per-laboratory basis, or using any other convenient distinction. The critical characteristic of this individual's accountability function is the responsibility of having an ongoing awareness of an agent's status within the laboratory. The accountable individual is responsible for providing information about how, when, where, and why assigned pathogens and toxins have been used, transported, or destroyed, and for maintaining current accountability (inventory) records.

It is important to realize that the idea of "Accountability" in MC&A is not to assign blame in case something goes missing, or an incident occurs with a strain over which someone had specific responsibility. Here are some thought questions regarding this issue: Why might assigning blame after an incident be a good idea? Why might it be a bad idea? How should you decide your policy?

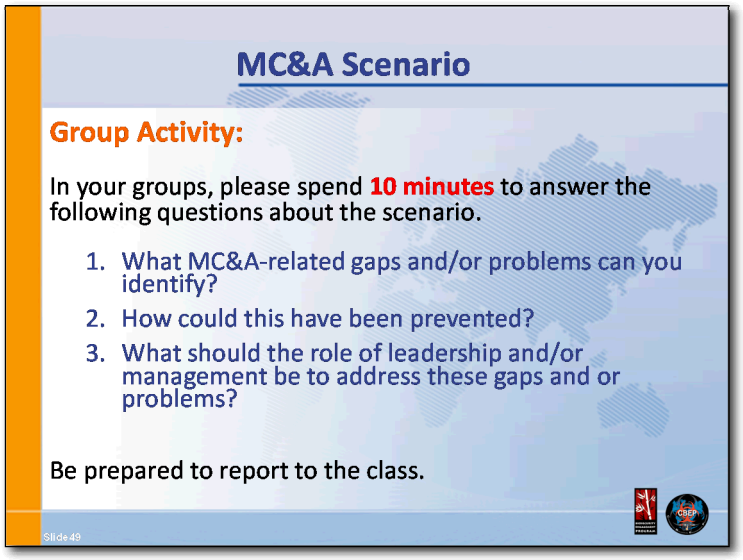
Accountable individuals are responsible for overseeing the work associated with their assigned pathogens or toxins. Any anomalies noted by the accountable individual should be reported to the appropriate officials promptly. The head of the facility should be responsible for ensuring that an appropriate accountable individual has been assigned to each dangerous pathogen or toxin located in the facility.

Material Control & Accountability

Slide 47



Slide 48



Material Control & Accountability

Small group activity (15 minutes).

Activity Instructions (to students)

- You have 10 minutes, in your groups, to read the scenario and answer the following questions.
- What MC&A-related gaps and/or problems can you identify?
- How could this have been prevented?
- What should the role of leadership and/or management be to address these gaps and or problems?
- Be prepared to report out to the class.

You have 15 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 and rationale.
- Continue around the room, asking other groups to report out, as time allows.
- Be sure to highlight any similarities, differences or unique answers.

Material Control & Accountability

Expected Responses

What MC&A-related gaps and/or problems can you identify?

- The agent could be high risk and was not subjected to strict inventory control measures.
- There was not an adequate inventory system in place
- Access to the agent may have been compromised but without and MC&A system we will never know.
- The accountable person had left the laboratory and accountability was not transferred to a new person

How could this have been prevented?

- With a MC&A system in place that covers all aspects discussed in the slides.

What should the role of leadership and/or management be to address these gaps and problems?

Institute policies that address the following:

- The accountable individual is responsible for ongoing awareness of an agent's status within the laboratory
- The accountable individual is responsible for providing information about how, when, where, and why assigned pathogens have been used, transported, stored, or destroyed
- Lab must maintain current inventory records
- There must be a procedure in place to report anomalies promptly
- Conduct performance reviews

New Responses from Students:

Material Control & Accountability

Slide 49

Ask students to REFLECT individually on the following question/statement:

How is Material Control & Accountability implemented in your laboratory?

Ask: Any questions on Material Control & Accountability?

Take a Break (10 minutes)

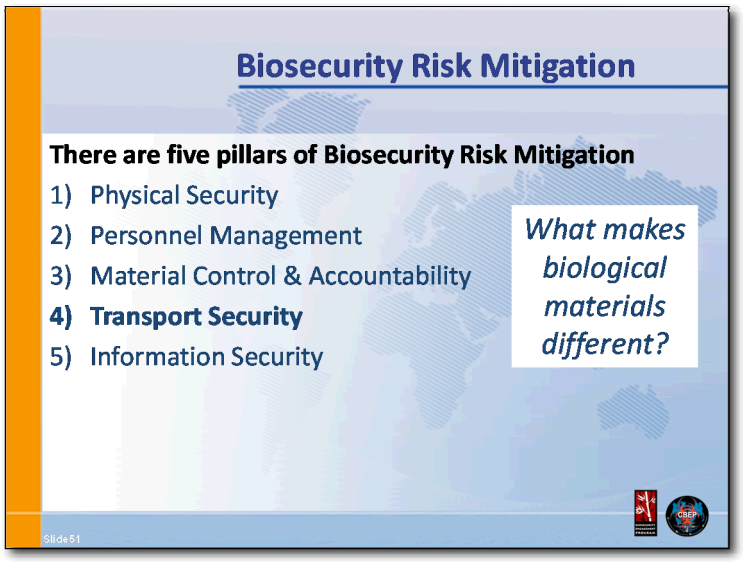
Time Check

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

Transition to Transport Security

Transport Security

Slide 50

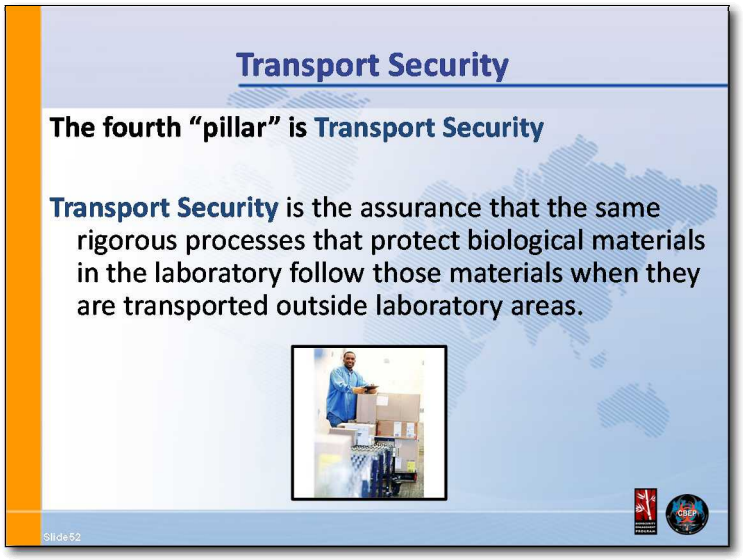


Lecture

A comprehensive biosecurity program must include a combination of all the pillars of Biosecurity Risk Mitigation. Now we will focus on the Transport Security component.

Transport Security

Slide 51



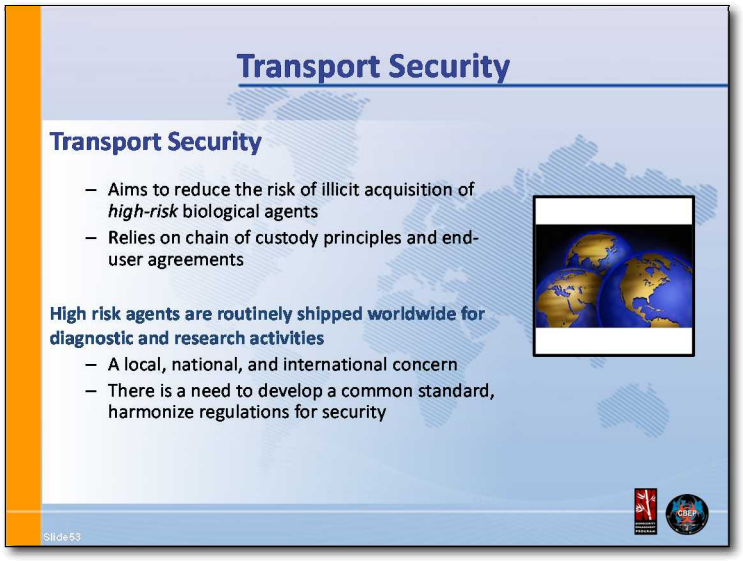
Background Information for Instructor

Transport security is a mechanism to implement MC&A while material is being transported between restricted areas to reduce the risks of theft or misuse. For example, we don't want to spend all of this effort protecting biological materials in the lab only to have an incident occur when the sample is being transported.

Limiting the amount of time that the biological agents are outside of restricted areas also reduces the opportunity for theft.

Transport Security

Slide 52



Background Information for Instructor

During the process of transportation, materials move outside of established restricted areas and may be more vulnerable to theft or tampering.

Accountability of the material, documentation, and oversight during the transport process are measures that improve biosecurity.

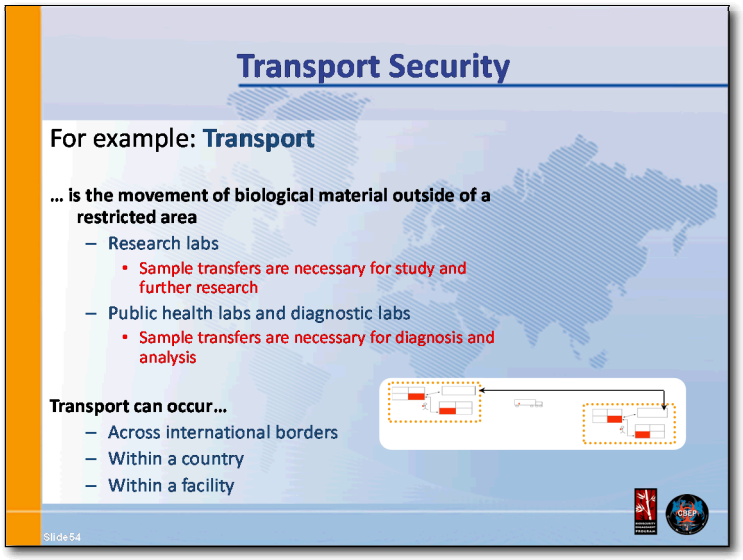
Release of a biological agent outside of the laboratory could be a local, national, and international concern – depending on the agent and the consequences of a release. Because of this international standards have been implemented to help reduce the risk of release during transport.

For example:

- Transport security mechanisms must coexist with a large body of safety regulations; must allow for the efficient transportation of all materials and must remain cost effective so as not to unduly hinder the research and diagnostic work.
- Quantity limitations also provide some security benefits.

Transport Security

Slide 53

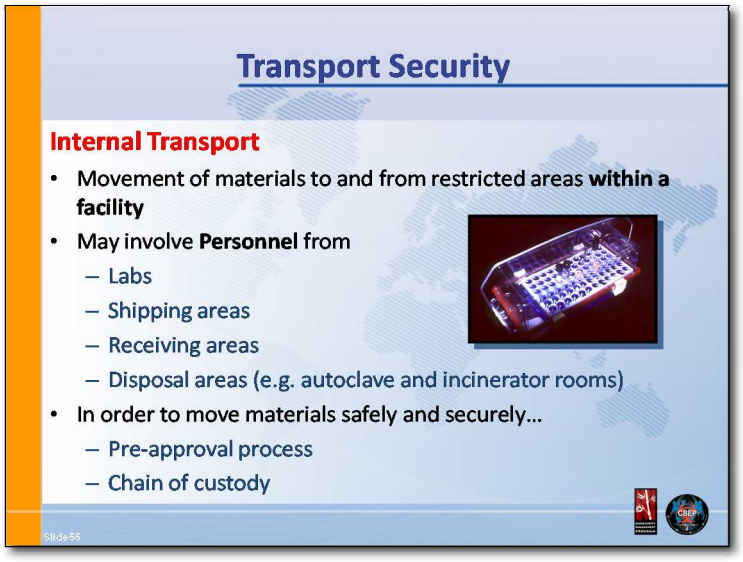


Background Information for Instructor

Transport can happen in a variety of contexts. Generally, it is movement of biological material outside of a restricted area. The restricted area is typically the laboratory. An example could be transport of a sample from the field (source of a disease outbreak) to a diagnostic public health laboratory, and then to a research laboratory for more specialized analysis. Transport can be within a facility, between facilities within a country, or internationally. Transport can also be grouped into internal and external transport. We will discuss both of these categories in more detail in the next few slides.

Transport Security

Slide 54



Transport Security

Background Information for Instructor

Internal transport is the movement of dangerous pathogens and toxins between restricted areas at a facility.

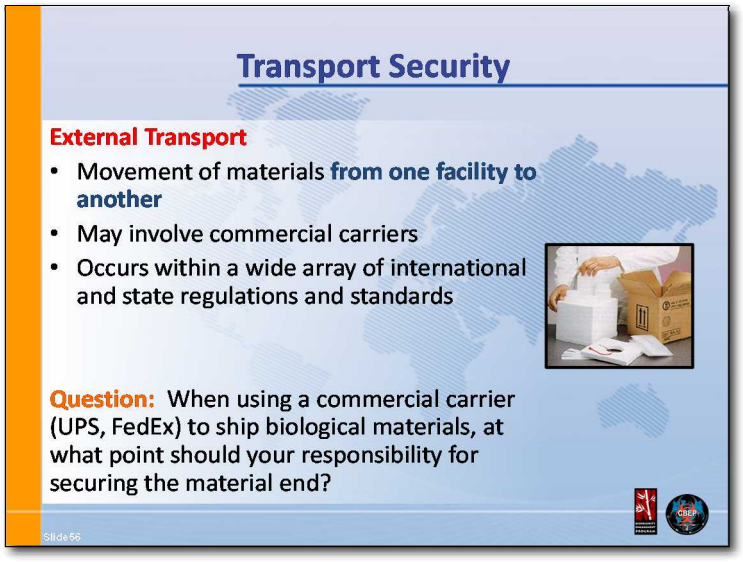
This type of transport typically involves an individual in the originating laboratory removing a sample from storage, walking it across the facility, and handing the sample to an individual in the receiving location. Then the receiving laboratory either uses the sample or places it in storage. Such movement may occur as laboratories exchange materials under study; internal transport also includes materials added or removed from the inventory as a result of shipping and receiving processes, or materials sent to disposal areas (e.g., autoclave and incinerator rooms).

Some key considerations when implementing a transport security program include:

- Determining at which point a diagnostic sample should be subject to internal or inter-facility transport security procedures.
- Who is responsible for preparing packages in accordance with all appropriate regulations – laboratory personnel or shipping department, or other.
- Whether biosafety and biosecurity measures are implemented upon arrival of a specimen at the facility if it is suspected of containing a dangerous biological agent or are they initiated after the sample is determined through confirmatory testing to be an agent that requires transport security.

Transport Security

Slide 55



Transport Security

Background Information for Instructor

External transport refers to the process of moving dangerous pathogens or toxins between facilities.

The first step in implementing security for external transport begins with confirming receiver eligibility and awareness, and securing the package for transport. For example, procedures should also be established so that an accountable institutional official is notified in advance that a shipment of dangerous biological materials will be received at the facility.This process likely includes some internal transport steps (e.g., to a shipping area or from a receiving area) in addition to relinquishing custody to a commercial carrier or courier before external transport actually happens. It is important to establish a change of command throughout the entire transport process. This includes, designating individuals who are responsible for package tracking and monitoring during the external transport as well as having a process to ensure notification to the sending facility that the material has been successfully received. There should also be procedures for reporting missing shipments of higher-risk agents to appropriate authorities.

In addition, the packaging should not attract any special attention; labels on the outside packaging should have only the minimum identifying information required by the commercial carrier and national and international regulations.

Transport Security

In plenary, ask students:

When using a commercial carrier (UPS, FedEx) to ship biological materials, at what point should your responsibility for securing the material end?

Expected Response:

Your responsibility does not end at any point in the process; instead the sender should still continue to monitor the progress of the shipment.

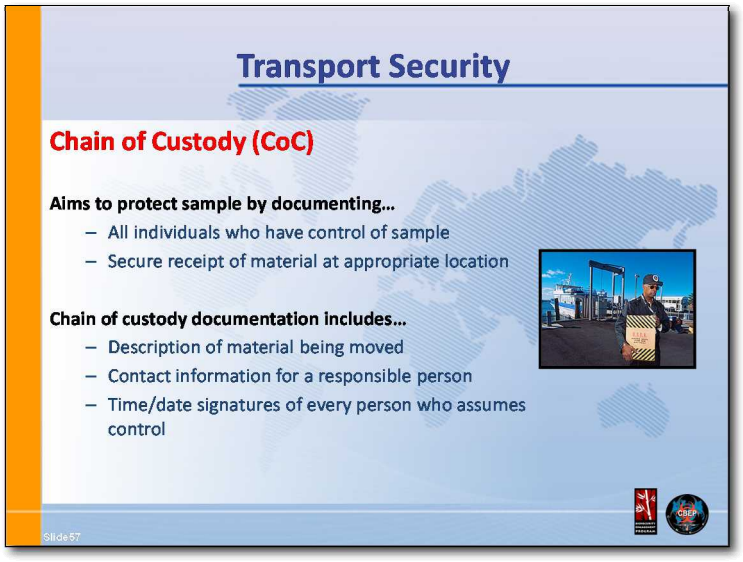
Here are some notes about carriers:

Security while the package is en-route begins with the selection of a reputable carrier. The opportunity for theft is greatly reduced by limiting exposure time to the commercial transport system. Although many commercial carriers provide tracking services, it should be recognized that these services are not real-time nor do they guarantee custody over a package at all times. However, tracking does provide information regarding the relative position of the package in the transport system and can facilitate creating a document trail for facilities.

It should be noted that a facility cannot guarantee or oversee the security of material outside of the facility but consideration of external security issues can limit the possibility of incidents. As warranted by the risk, additional procedural steps can be taken by shipping and receiving facilities to exercise due diligence during all three stages of external transport: pre-shipment, en-route, and receipt.

Transport Security

Slide 56



Transport Security

Background Information for Instructor

Despite the type of transport, all transport should adhere to a Chain of Custody. Chain of custody refers to the process employed to document who has control of a sample and when. The chain-of-custody process documents that an accountable individual has control over the integrity of the packaged material, and that secure receipt of the material has occurred at the appropriate facility location.

Chain-of-custody documentation accompanies the material during transport and includes the name and quantity of material being moved, the shipping and consignee contact information (or laboratory contact information as applicable), and time and date signatures of every individual who assumes control of the material en-route (e.g., those who initiate delivery, package, or relinquish custody).

The chain-of-custody process also documents any situation in which an individual assumes custody on behalf of another individual. If an authorized individual is not able to ensure custody of the package, then the package can be controlled in a restricted area or within an access-controlled cage or freezer.

Chain of custody can be achieved via many mechanisms, including paper, where each individual signs a physical document, or personal digital assistant (PDA) scanners.

Unfortunately, a chain of custody does not guarantee that a sample will not be stolen, but it does provide traceability as well as raise the threshold for theft by introducing a degree of accountability in the transfer process.

Transport Security

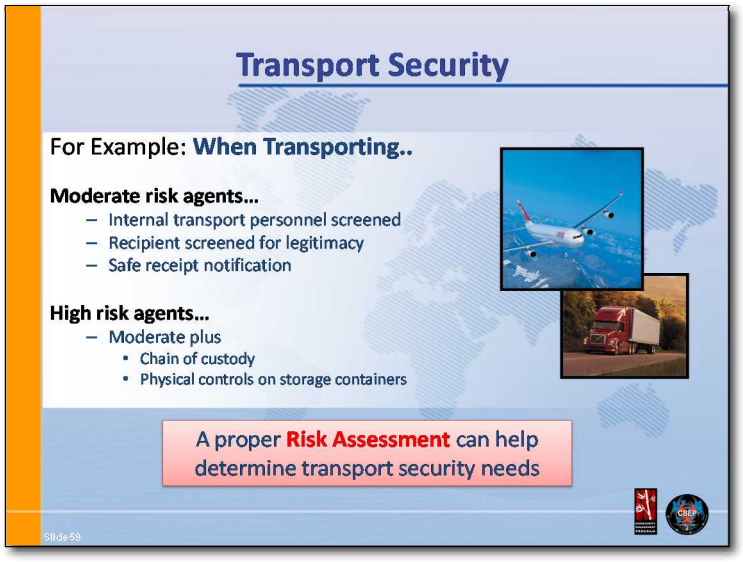
Slide 57

Background Information for Instructor

This slide summarizes the main objectives and the take home messages with regard to transport. It may be used to provide an overview, some guidance and also to solicit any thought and viewpoints.

Transport Security

Slide 58



Transport Security

Background Information for Instructor

A risk assessment will determine transport security needs. These may fall into categories depending on the risk associated with the agent. Listed are some recommendations for risk mitigation efforts to promote safe and secure transport of biological material. For example, for higher-risk materials, a facility may decide that transport must be pre-approved by a designated institutional responsible official or biosafety officer (BSO). In addition, prior to approving the transport, the individual ensures that a new accountable individual is identified at the recipient laboratory or verify that appropriate shipping or destruction documentation is maintained.

Some notes on this topic include:

Since materials may be vulnerable to theft while outside of restricted areas, facilities need to demonstrate prudent and sufficient stewardship of these materials during transport, with more stringent measures in place for the transport of higher-risk materials.

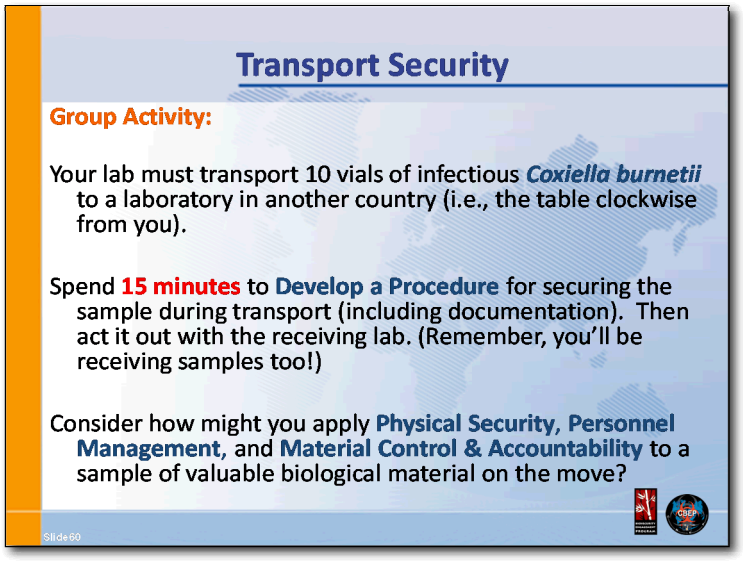
Facilities should recognize that laboratory personnel are not necessarily the only ones with unescorted access to dangerous pathogens and toxins during transport. Transport protocols can be analyzed to determine who may have access to such materials, such as dedicated delivery people.

Analysis of transport processes may identify areas that are used for temporary storage, such as shipping and receiving offices or loading docks. Controls should be implemented in these areas at a level equivalent to the restricted areas where the material is stored or used.

Transport of materials should also be integrated into the MC&A protocols.

Transport Security

Slide 59



Transport Security

Small group activity (20 minutes).

Activity Instructions (to students)

1. Spend 15 minutes to read the scenario and develop a procedure for securing the sample during transport (including documentation). Then act it out with the receiving lab. (remember, you'll be receiving samples too!)
2. Also consider how might you apply Physical Security, Personnel Management, and Material Control & Accountability to a sample of valuable biological material on the move?

You have 20 minutes to complete this activity

Directions for Instructor:

- After 15 minutes, ask the students to stop working on the exercise
- Have the students pair up with another group and act out the whole procedure for transporting a sample. The groups should take turns acting as the sender and receiver.
- Ask students to report out how the procedures went, making sure to highlight any challenges and proposed solutions. Continue around the room, asking other groups to report out, as time allows.
- Be sure to highlight any similarities, differences or unique answers.

Transport Security

Expected Responses

Students should incorporate all of the tools and concepts provided in the previous slides.

- Notifications
- Chain-of-custody
- Documentation
- Preapproval
- Securing samples in transport container
- Selecting a credible and proficient courier

New Responses from Students:

Slide 60

Transport Security

Ask students to REFLECT individually on the following question/statement:

How are biological materials secured in your laboratory during transport?

Ask: Any questions on Transport Security?

Take a Break (10 minutes)

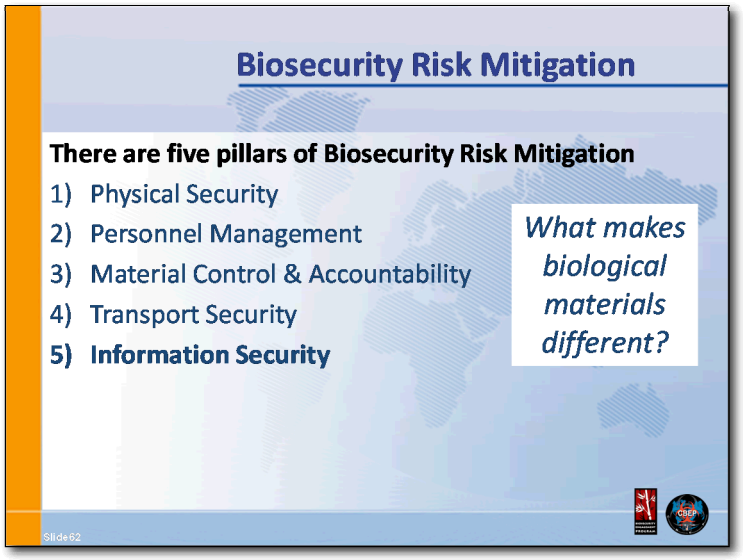
Time Check

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

Transition to Information Security

Information Security

Slide 61

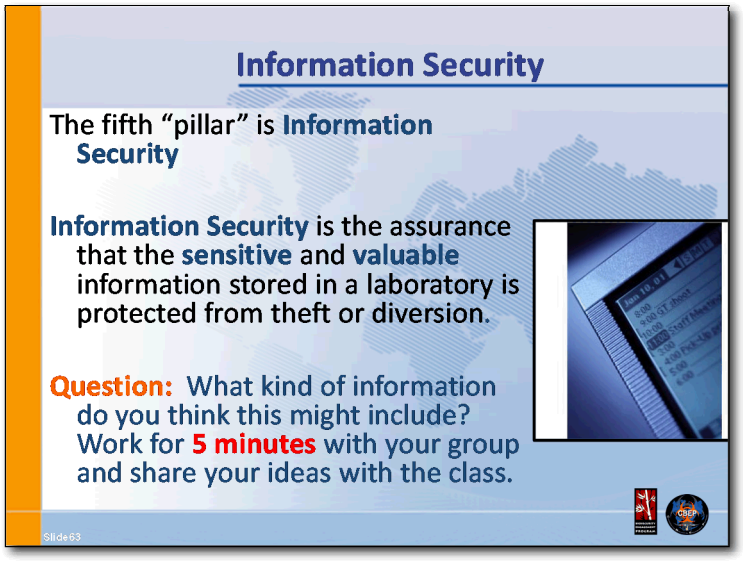


Lecture

A comprehensive biosecurity program must include a combination of all the pillars of Biosecurity Risk Mitigation. Now we will focus on the Information Security component.

Information Security

Slide 62



Background Information for Instructor

Information security is a set of tools and practices used to protect sensitive information. Overall there is a need to protect information relating to valuable biological materials (VBM), which would allow an adversary to gain access to the laboratory. This type of protection is very similar to that already followed for personal and financial information.

Information Security

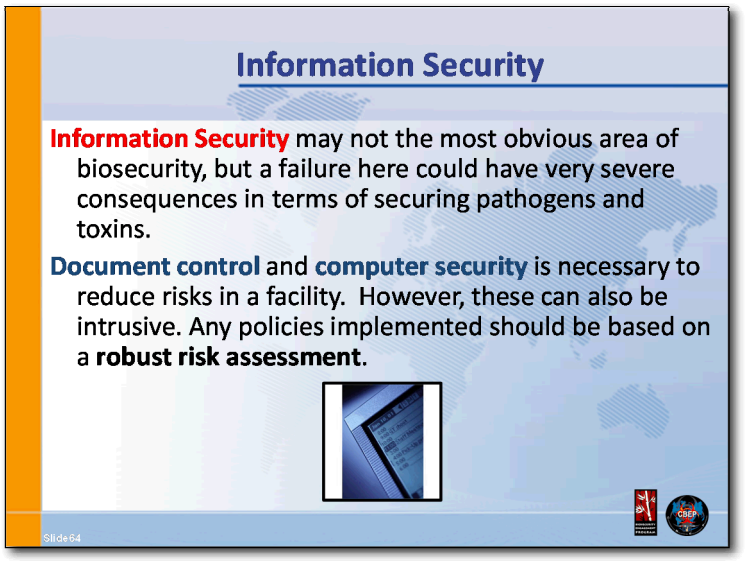
In plenary, ask students:

What kind of information do you think this might include?

Expected Responses:

- Location/inventory of sensitive agents, materials and equipment
- Lab protocols
- Patents
- Data
- Personnel records
- Transportation records
- Sensitive security information

Slide 63

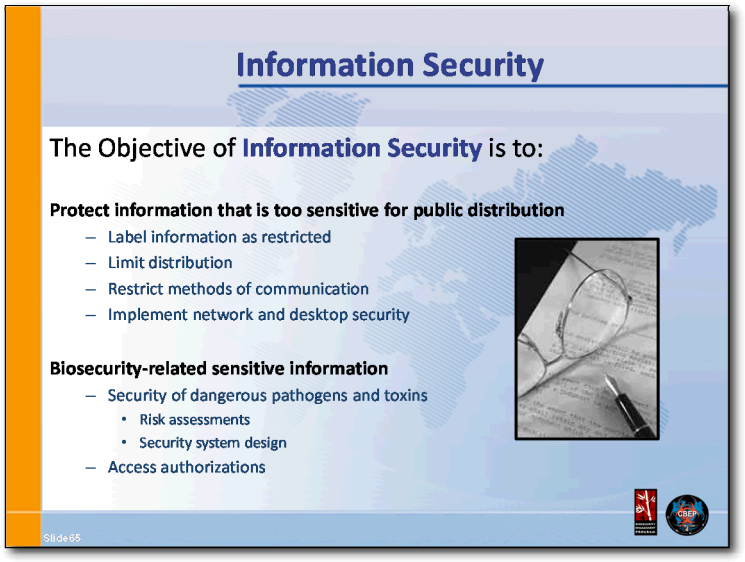


Information Security

Background Information for Instructor

Protecting sensitive information from release is a security measure because release of this information could aid an individual's efforts to steal protected biological agents by indicating how to circumvent the laboratory biosecurity system. Sensitive security information may be connected to any of the elements of laboratory biosecurity. For example any information regarding physical security plans, user-level access, or other details of the physical security system should be considered sensitive. Information security is devoted to protecting information that may be considered sensitive, particularly sensitive security-related information. This could also include data on risk assessments. Information security relies heavily on document control and computer security.

Slide 64



Information Security

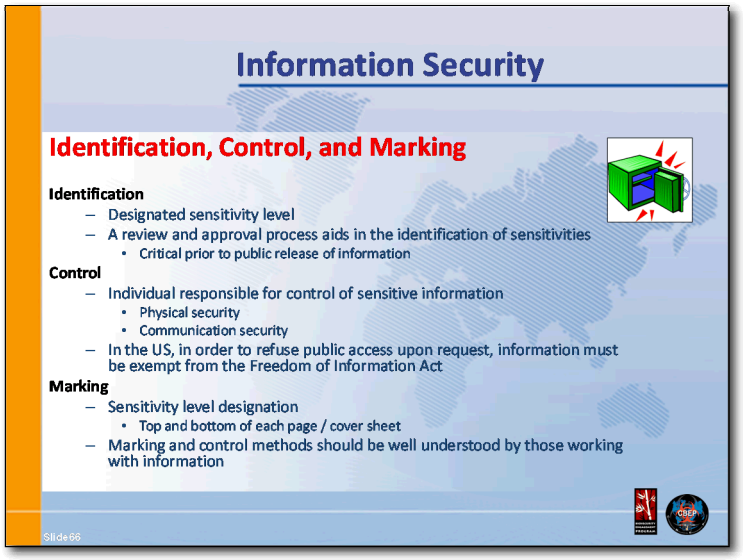
Background Information for Instructor

Recommendations for mitigation measures that can be taken to protect information that is too sensitive for public distribution include:

- Limit/restrict communication and methods of communication to secure and approved methods.
- Transmission of moderate or highly sensitive information should occur only via approved methods
- Mail, email, or fax security is required
- Limited discussions in open areas
- Information should only be reproduced when needed and each copy must be controlled as the original. Reproduction should also be observable.
- Measures encompass handling, storing, transmitting, and destroying information.
    - This includes shredding or burning. A hard-drive wiping program provides a similar level of destruction for electronically stored sensitive information.
    - Electronic storage devices can be destroyed through physical damage to the point of inoperability via shredding, degaussing, melting, or other such methods before disposal.

Information Security

Slide 65



Background Information for Instructor

Identifying materials with a designated sensitivity level is a way to limit unauthorized distribution. For example,

- Low (open or public information)
- Moderate (limited access information)
- High (exclusive or strict access information)

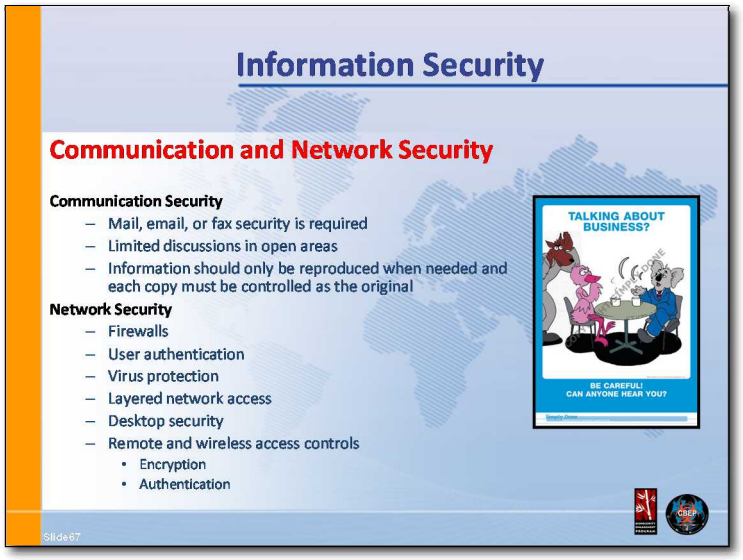
In addition, a review and approval process aids in the identification of sensitivities before distribution occurs. Further, it is important to have designated individuals who are responsible for controlling the information.

All individuals handling sensitive information should have appropriate training. Having a clear process for determining what information can be shared with whom can be a significant benefit to laboratory biosafety and the institution as a whole. In some cases, without such a process, employees can self-censor information because they do not know what is acceptable to release from a legal and institutional perspective.

The first step in providing information security is identifying information that is sensitive. This can be achieved through using consistent marking methods.

Information Security

Slide 66



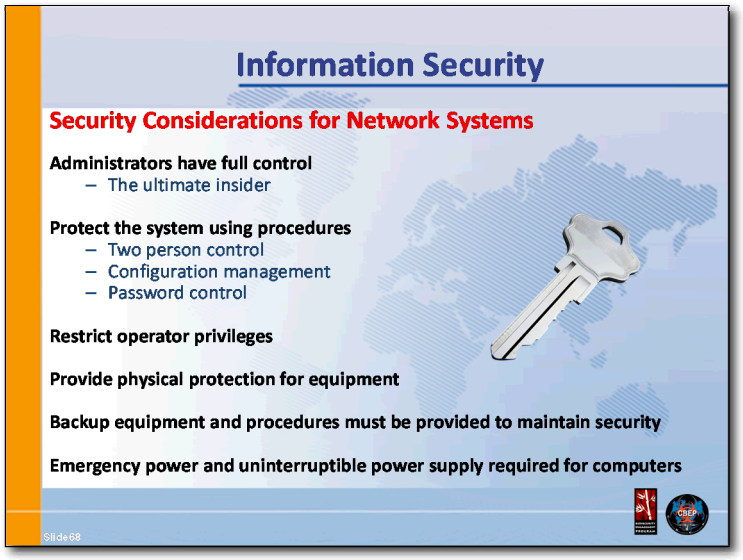
Background Information for Instructor

Much of the sensitive information found in a laboratory is found in electronic formats on stand-alone computers and computer networks throughout the facility. Depending on the risk assessment it may be appropriate to store information that is critical to security (e.g., physical security systems, dangerous pathogen inventories) on standalone computers or isolated networks within restricted areas to limit the risk of compromise.

In addition, all elements of the network (routers, servers, web servers, web applications, domains, firewalls, wireless local area networks, and remote access) need to be assessed from a security perspective. Strong passwords, desktop management of upgrades and patches, and virus protection are all important aspects of desktop security measures for any computer with sensitive information or with access to a network that contains sensitive information.

Information Security

Slide 67



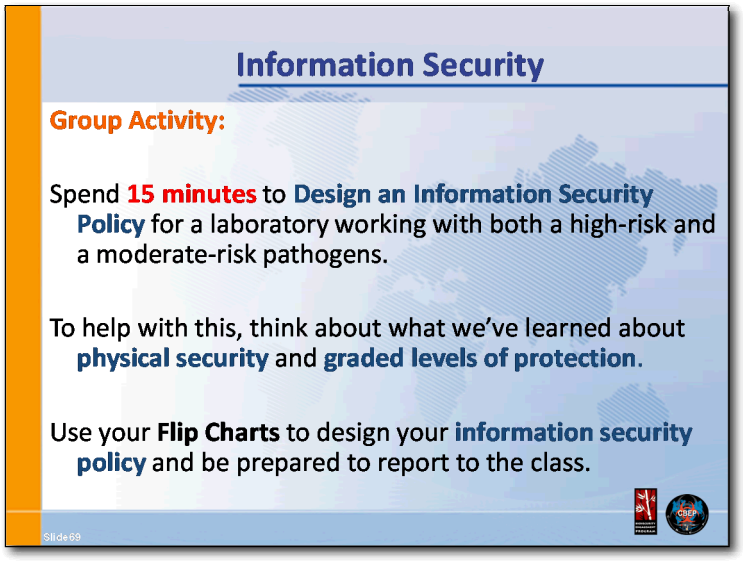
Background Information for Instructor

Additional mitigation measures to protect information include establishing a robust network management system. For example, the network on which all information is transmitted should be protected. This includes infrastructure, servers, remote access, and wireless connections. In addition, any individual with root administrative access to the administrative or security network needs to be aware of information sensitivity levels and cognizant of any actions taken in the handling and protection of that information.

Training and policy controls should be implemented for individuals with root access to these systems. Individuals with root access should be screened to the highest level associated with the information or controls that root access provides to them.

Information Security

Slide 68



Information Security

Small group activity (20 minutes).

Activity Instructions (to students)

- Spend 15 minutes to design an information security policy for a laboratory working with both moderate-risk and high-risk pathogens.
- To help with this, think about what we've learned about physical security and graded levels of protection.
- Use your Flip Charts to design your information security policy 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 5-minute plenary discussion. Begin by asking for one group of students to report their information security system and have the students elaborate on specific components.
- Be sure to highlight any similarities, differences or unique answers.

Information Security

Expected Responses

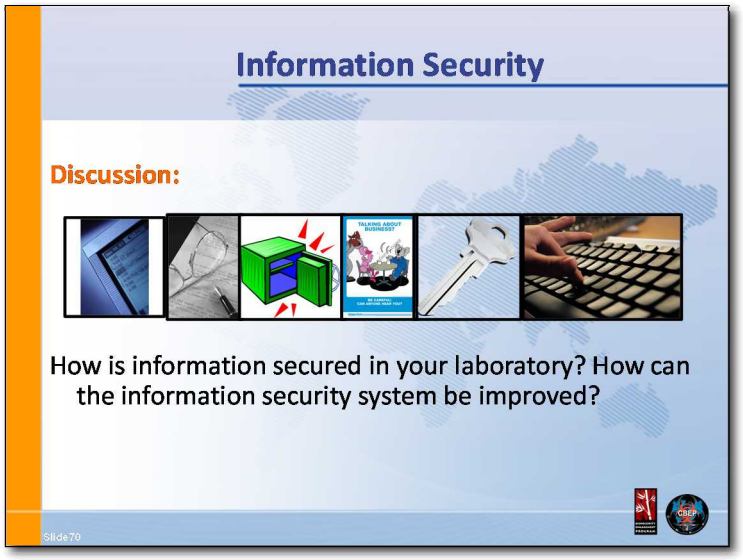
Students should incorporate all of the tools and concepts provided in the previous slides.

- Computer network security
- Firewall protection
- Use of passwords
- Graded level of security of information
- Designating responsible individuals
- Incorporate into SOPs
- Identifying and marking sensitive documents
- Training on limiting distribution and communication of sensitive information
- Document control
- Notifications
- Chain-of-custody
- Documentation
- Preapproval

New Responses from Students:

Information Security

Slide 69



Ask students to REFLECT individually on the following question/statement:

How is information secured in your laboratory? How can the information security system be improved?

Ask: Any questions on Information Security?

Take a Break (10 minutes)

Time Check

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

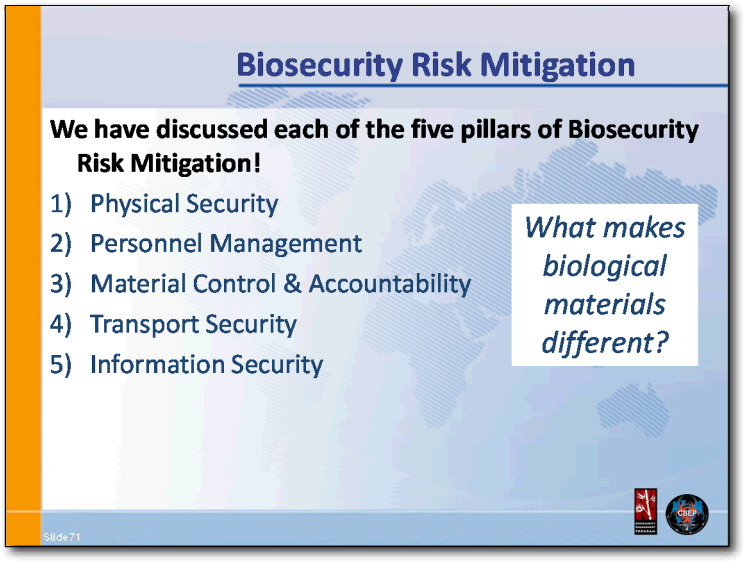
Transition to Security Awareness

Information Security

Take a Break (15 minutes)

Security Awareness

Slide 70

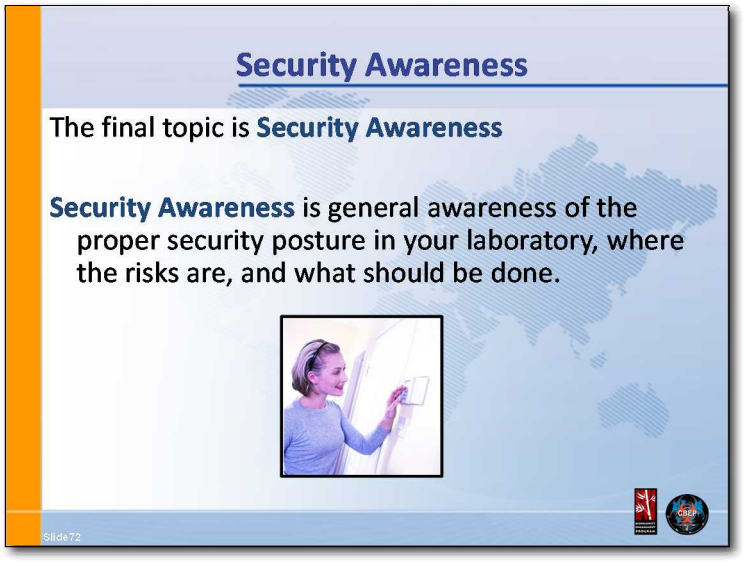


Lecture

We have completed our review of each of the five pillars of Biosecurity Risk Mitigation. Remember that a comprehensive biosecurity program must include a combination of all the pillars of Biosecurity Risk Mitigation.

Security Awareness

Slide 71



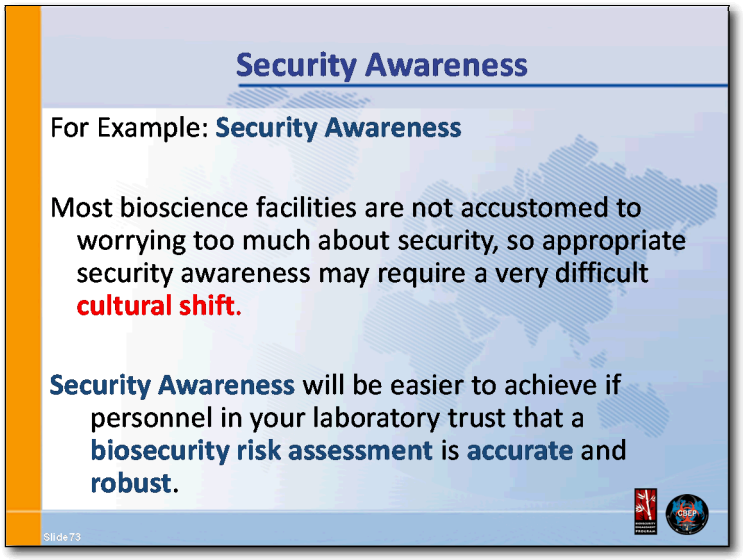
Background Information for Instructor

Whereas, security awareness is not considered a separate pillar of Biosecurity Risk Mitigation, it definitely ties into the objectives of each pillar.

Security awareness is the knowledge and attitude members of an organization (the lab management and workers) possess regarding the protection of the physical and, especially, information assets of that organization. It can also be described as an overall recognition of security concerns and the appropriate response to decrease biosecurity risk inside and outside the laboratory.

Security Awareness

Slide 72



Background Information for Instructor

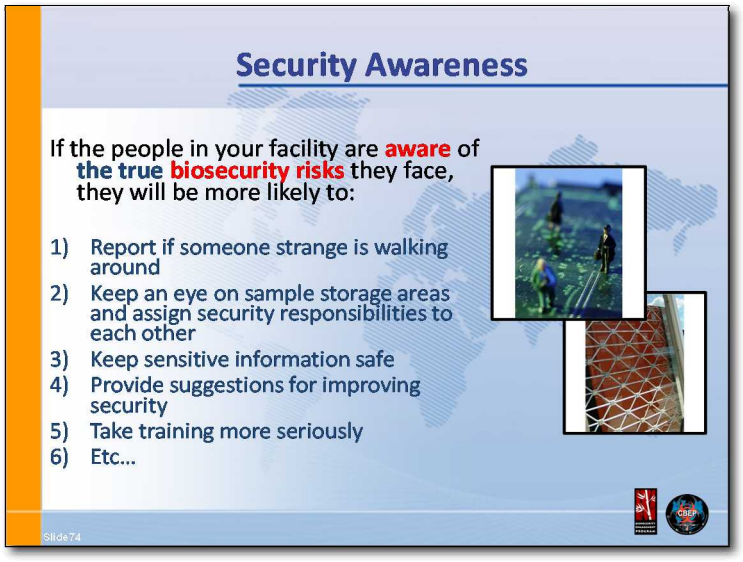
There are many factors that contribute to an overall dedication security awareness in the laboratory. Biosecurity awareness needs to be developed over time for it to set into the overall culture of the laboratory.

To achieve this goal, security awareness training as well as cooperation and understanding of laboratory activities potentially affected by lapses in biosecurity helps to create awareness and balance perceptions on what is occurring in the laboratory. The focus of Security Awareness training should be to achieve a long-term shift in the attitude of employees towards security, whilst promoting a cultural and behavioral change within an organization.

Overall, developing a culture of security awareness is everyone's responsibility and requires a real commitment to biosecurity.

Security Awareness

Slide 73



Security Awareness

Background Information for Instructor

Being security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization. This includes an overall responsibility of keeping pathogens, staff and personnel, the community outside the lab and the environment safe from harm.

In addition to the items listed on the slide, security aware individuals should know the following:

1. The nature of sensitive material and physical assets they may come in contact with.
2. Employee and contractor responsibilities in handling sensitive information, including review of employee nondisclosure agreements.
3. Requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction.
4. Proper methods for protecting sensitive information on computer systems, including password policy and use of two-factor authentication.
5. Other computer security concerns, including malware, phishing, social engineering etc.
6. Workplace security, including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.
7. Consequences of failure to properly protect information, including potential loss of employment, economic consequences to the firm, damage to individuals whose private records are divulged, and possible civil and criminal penalties.

Security Awareness

Slide 74

Security Awareness

Small group activity (10 minutes).

Activity Instructions (to students)

- Consider how might security awareness tie into the five pillars of biosecurity we have already discussed?
- Have each group pick one of the “pillars” and answer the above question.
- Work for 5 minutes with your group and share your ideas with the class.

You have 10 minutes to complete this activity

Directions for Instructor:

- After 5 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 answer to the rest of the class.
- Be sure to highlight any similarities, differences or unique answers.

Security Awareness

Expected Responses

Students should incorporate all of the tools and concepts provided in the previous slides.

Physical Security

- Awareness of where restricted areas are located and who is authorized to be in those areas.
- Understanding of access controls and how the principals of detection, delay, and response aid the objectives of physical security.

Personnel Management

- Awareness of others in the workplace, in terms of promoting factors that contribute to a productive work environment and alerting management if others break policy.

Material Control & Accountability

- Awareness of samples and alerting the appropriate people if a sample is missing.
- Awareness that samples are stored in a location that is appropriate to the level of risk associated with those samples.

Transport Security

- Awareness of the recipient, sender and anyone involved in the transport of biological samples.
- Awareness that security efforts must be implemented even during transport.

Information Security

- Awareness of alerting others if a suspected breach of information security is suspected.
- Awareness of the sensitivity associated with laboratory documents and how to label them accordingly.

New Responses from Students:

Security Awareness

Slide 75

Ask students to REFLECT individually on the following question/statement:

How might you promote a culture of increased security awareness in your laboratory?

Ask: Any questions on Information Security?

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 Review

Review

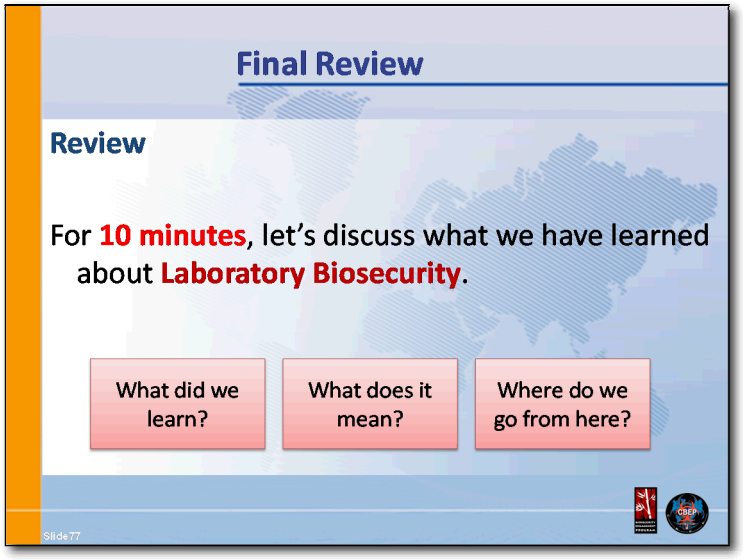
Goal

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

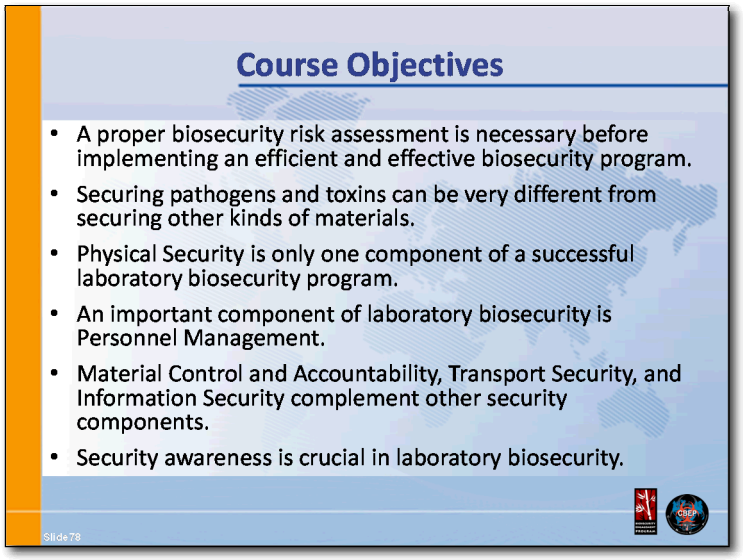
Allow 20 minutes to get through the Review section.

Slide 76



Review

Slide 77



Review Key Messages

Include discussion on how activities/examples relate to the Key Messages of the course and how the messages can be applied.

1. To learn how to protect biological agents and toxins in the laboratory from loss, theft, or misuse.

2. A proper biosecurity risk assessment is necessary before implementing an efficient and effective biosecurity program.

3. Securing pathogens and toxins can be very different from securing other kinds of materials.

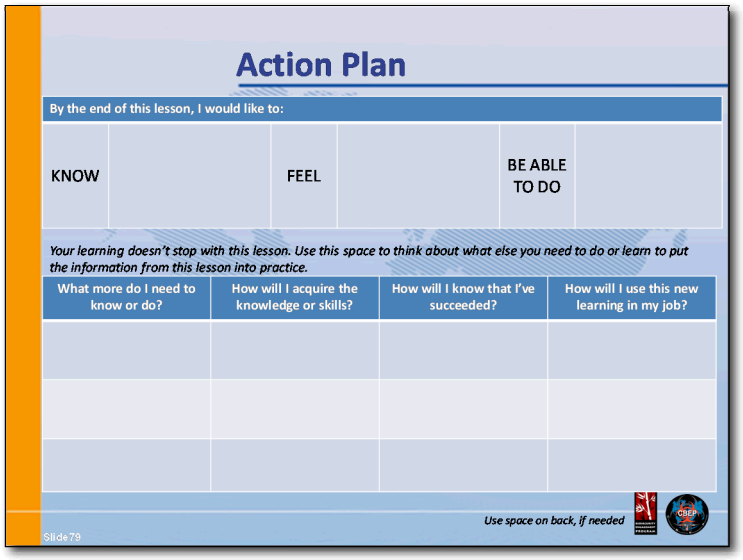
4. Physical Security is only one component of a successful laboratory biosecurity program.

5. Material Control and Accountability, Transport Security, and Information Security complement other security components.

6. Security awareness is crucial in laboratory biosecurity.

Review

Slide 78



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

Slide 79

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).