GBRMC

Basic Features & Maintenance for Physical and Information Security Measures

Student Guide

2017

GLOBAL BIORISK MANAGEMENT CURRICULUM


Basic Features & Maintenance for Physical and Information Security Measures
2017
GBRMC
GLOBAL BIORISK MANAGEMENT CURRICULUM

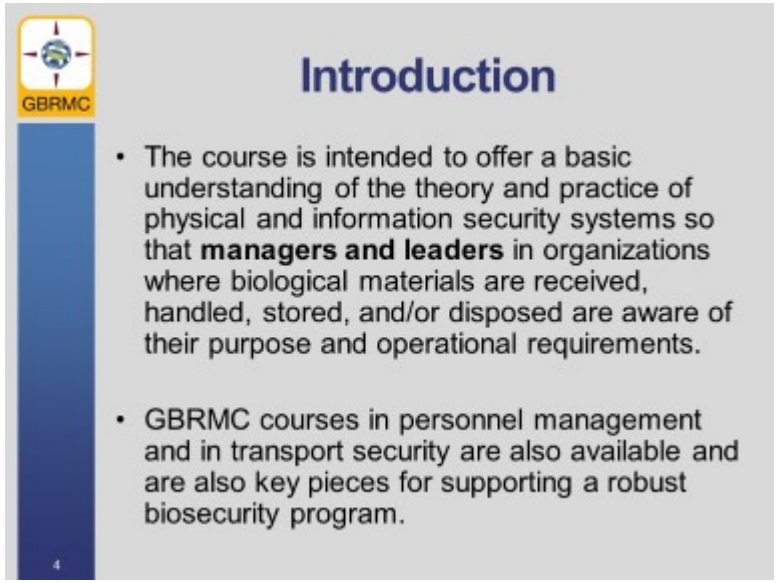

GBRMC
Introductions
• Trainers
• Students
– Your name?
– Where are you from?
2

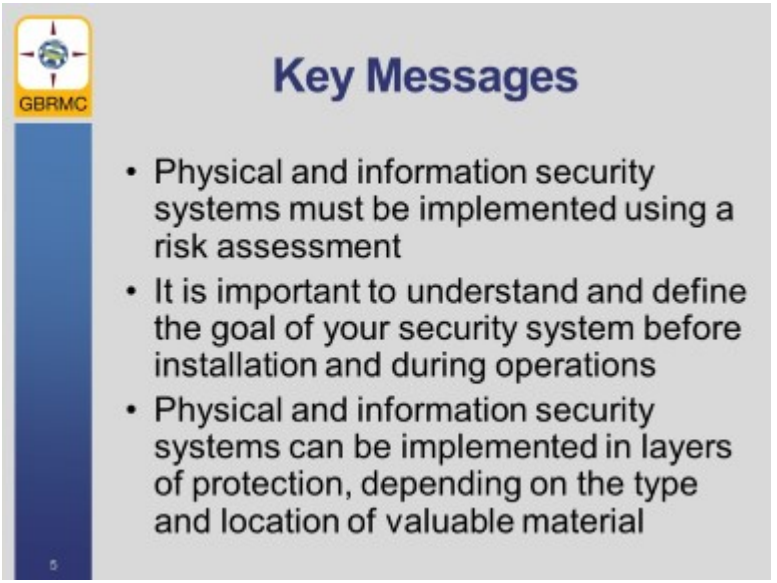
Action Plan

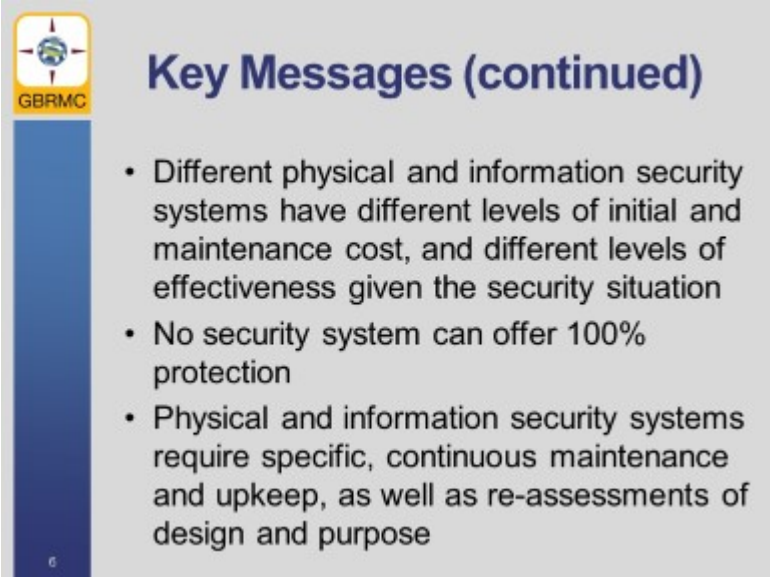
By the end of this lesson, I would like to:					
KNOW		FEEL		BE ABLE TO DO	

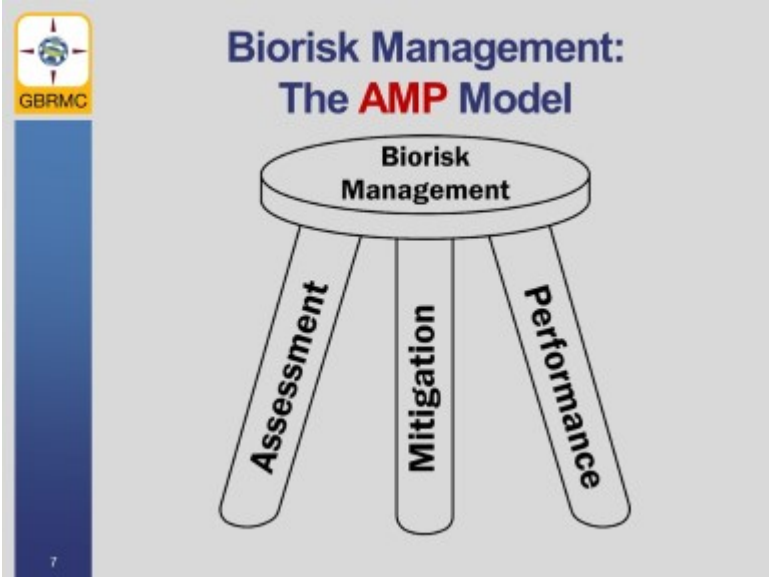
Your learning doesn't stop with this lesson. Use this space to think about what else you need to do or learn to put the information from this lesson into practice.

What more do I need to know or do?	How will I acquire the knowledge or skills?	How will I know that I've succeeded?	How will I use this new learning in my job?


GBRMC
Introduction
• The course is intended to offer a basic understanding of the theory and practice of physical and information security systems so that **managers and leaders** in organizations where biological materials are received, handled, stored, and/or disposed are aware of their purpose and operational requirements.
• GBRMC courses in personnel management and in transport security are also available and are also key pieces for supporting a robust biosecurity program.
4


GBRMC
Key Messages
• Physical and information security systems must be implemented using a risk assessment
• It is important to understand and define the goal of your security system before installation and during operations
• Physical and information security systems can be implemented in layers of protection, depending on the type and location of valuable material
5


GBRMC
Key Messages (continued)
• Different physical and information security systems have different levels of initial and maintenance cost, and different levels of effectiveness given the security situation
• No security system can offer 100% protection
• Physical and information security systems require specific, continuous maintenance and upkeep, as well as re-assessments of design and purpose
6


GBRMC
Biorisk Management: The AMP Model
Biorisk Management
Assessment
Mitigation
Performance
7

Key Components of Biorisk Management

- Biorisk **Assessment**
  - Process of identifying the hazards and evaluating the risks associated with biological agents and toxins, taking into account the adequacy of any existing controls, and deciding whether or not the risks are acceptable

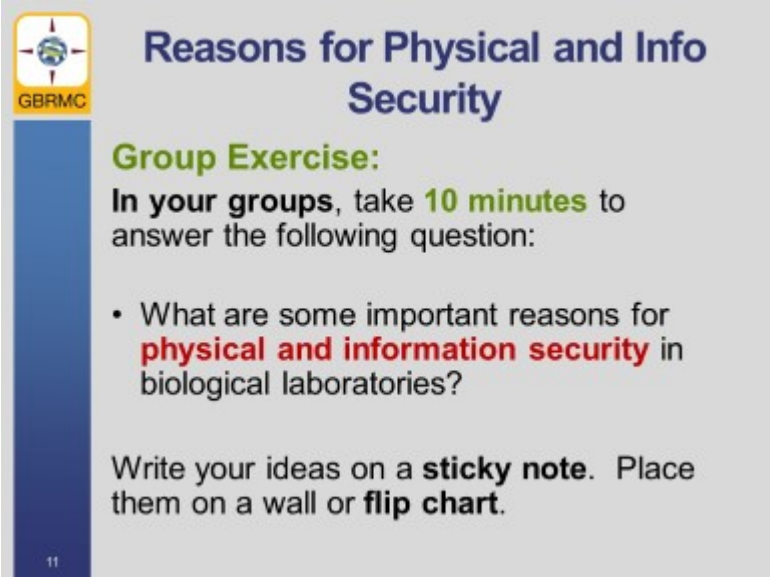
8

Key Components of Biorisk Management

- Biorisk **Mitigation**
  - Actions and control measures that are put into place to reduce or eliminate the risks associated with biological agents and toxins

9

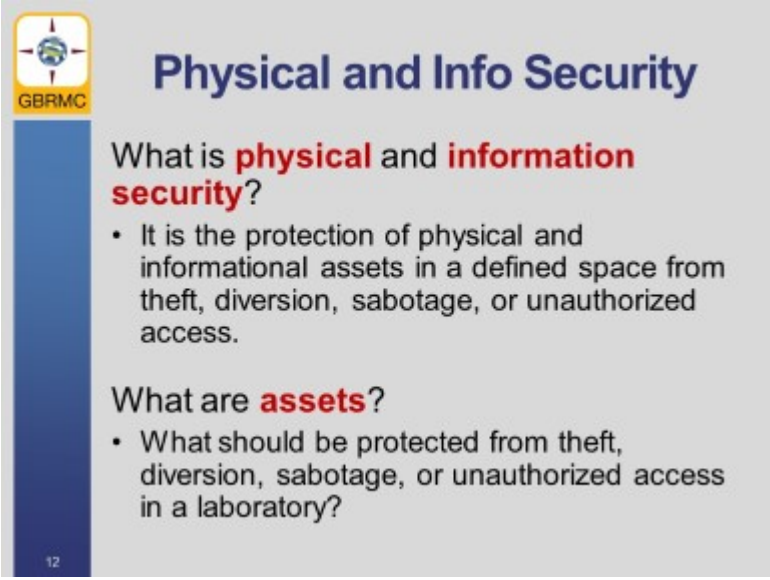

GBRMC
Key Components of Biorisk Management
• Biorisk **Performance**
– Improving biorisk management by recording, measuring, and evaluating organizational actions and outcomes to reduce biorisk.
10



What are some important reasons for physical and information security in bioscience laboratories?

Physical security:

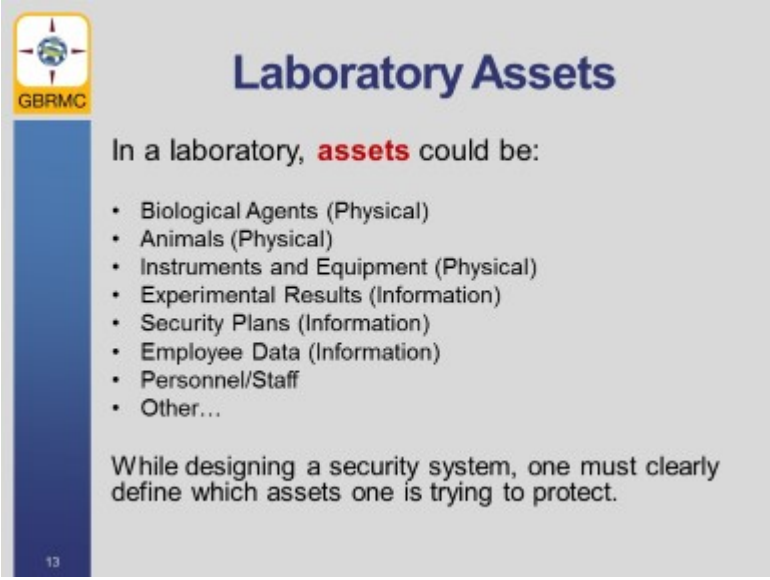
Information security:



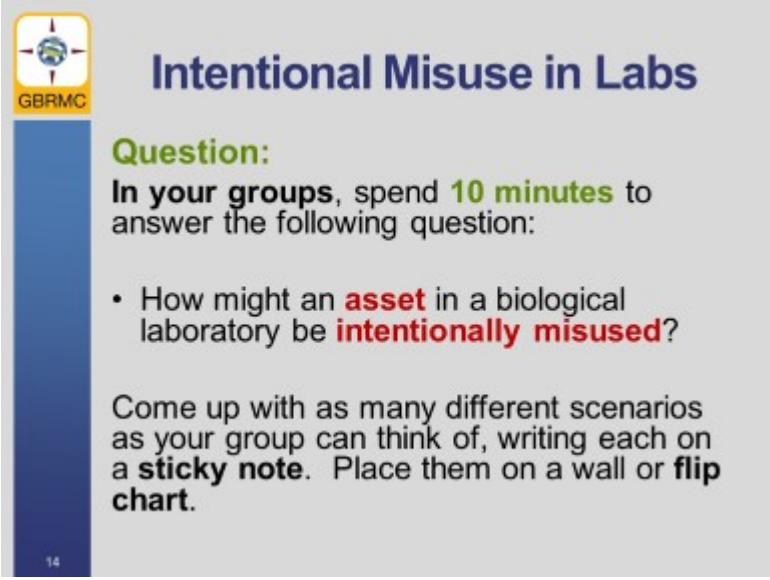
What is physical security?

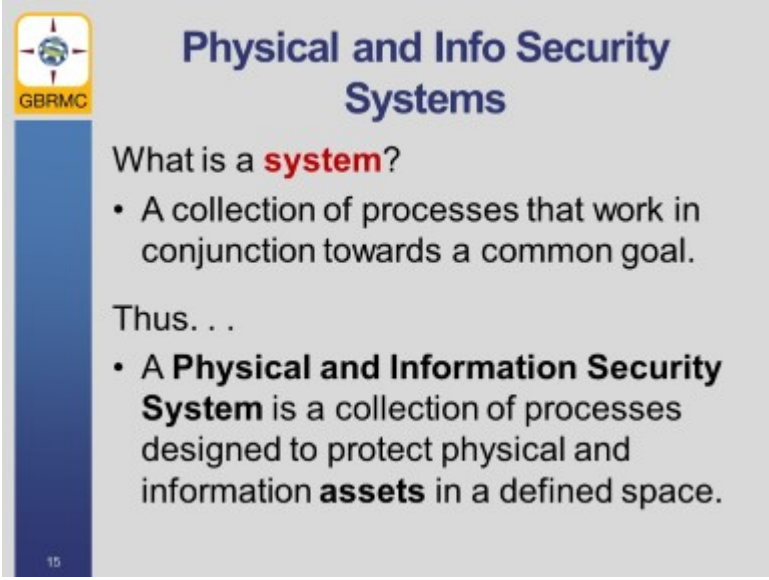
What is information security?

What are “assets” when thinking about security issues?



Other assets?

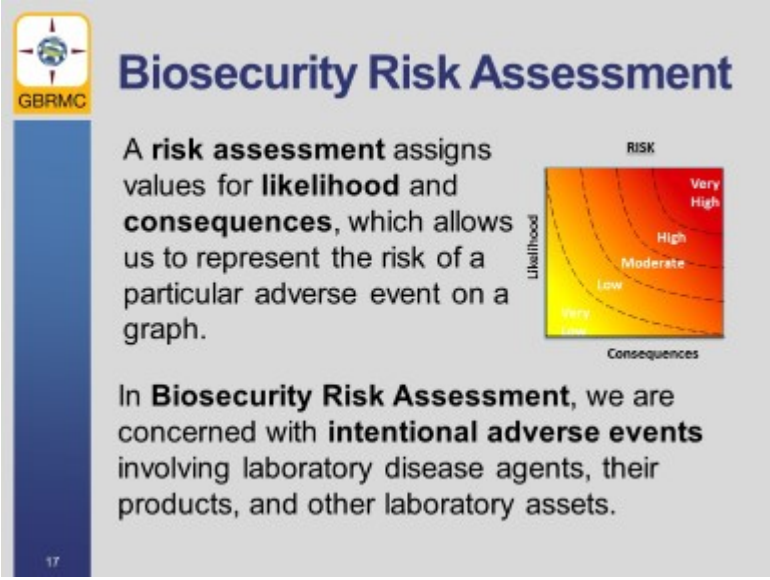

GBRMC
Intentional Misuse in Labs
Question:
In your groups, spend 10 minutes to answer the following question:
• How might an asset in a biological laboratory be intentionally misused?
Come up with as many different scenarios as your group can think of, writing each on a sticky note. Place them on a wall or flip chart.
14


GBRMC
Physical and Info Security Systems
What is a system?
• A collection of processes that work in conjunction towards a common goal.
Thus. . .
• A Physical and Information Security System is a collection of processes designed to protect physical and information assets in a defined space.
15

Risk is a function of likelihood and consequences. In order to determine a biosecurity risk we must assess both the likelihood of a biosecurity event as well as the magnitude of its consequences.

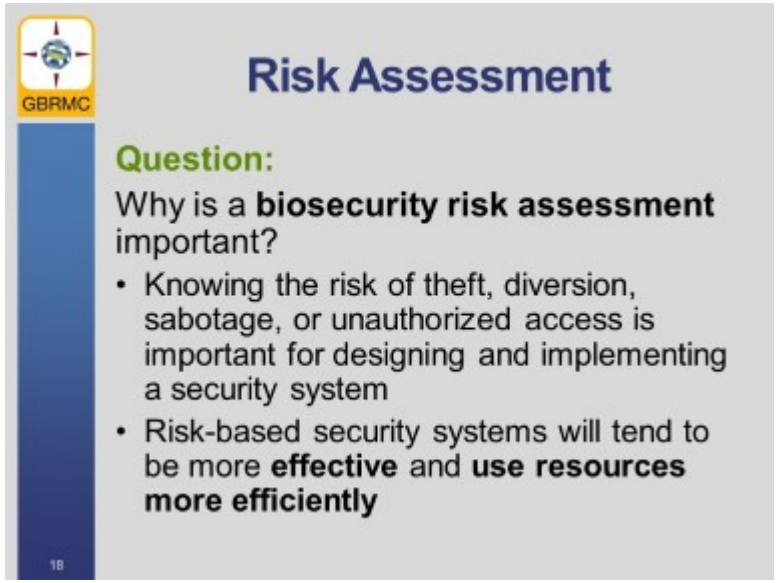
Why is a risk assessment essential to designing and implementing a security system?

Why are risk-based systems more effective and use resources more efficiently?



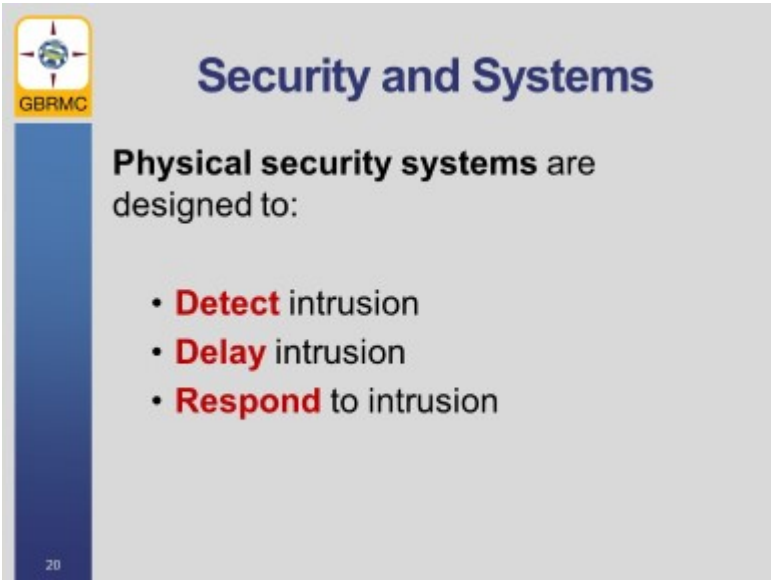
A graph of likelihood vs. consequence can help you visually map out different risks for different scenarios. . .

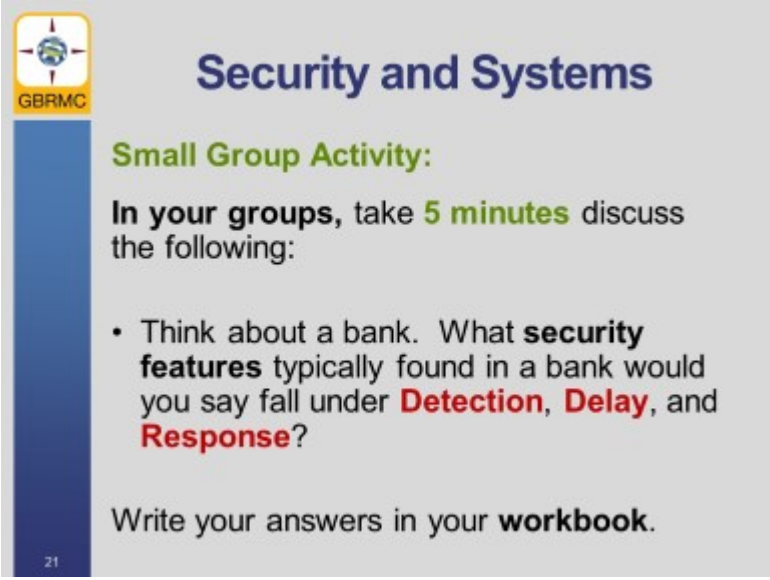
Being able to chart and visualize risks in a similar fashion can allow you to prioritize responses to different risks.

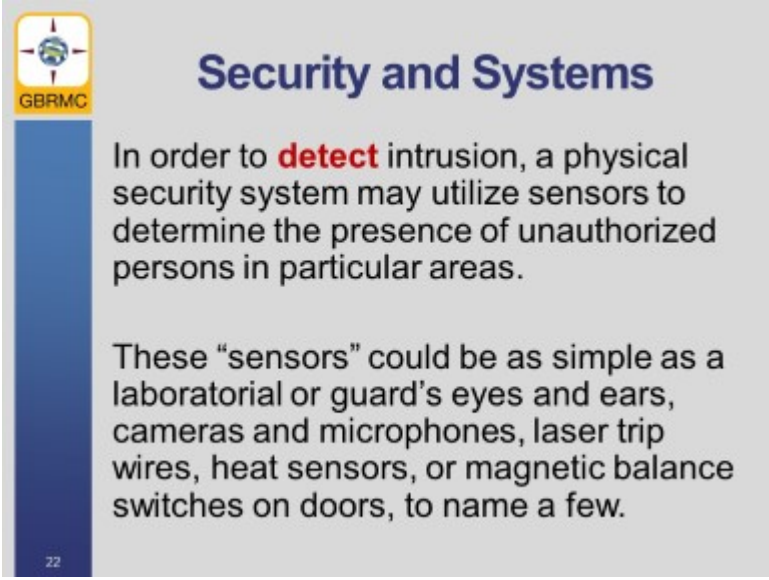

GBRMC
Risk Assessment
Question:
Why is a biosecurity risk assessment important?
• Knowing the risk of theft, diversion, sabotage, or unauthorized access is important for designing and implementing a security system
• Risk-based security systems will tend to be more effective and use resources more efficiently
18

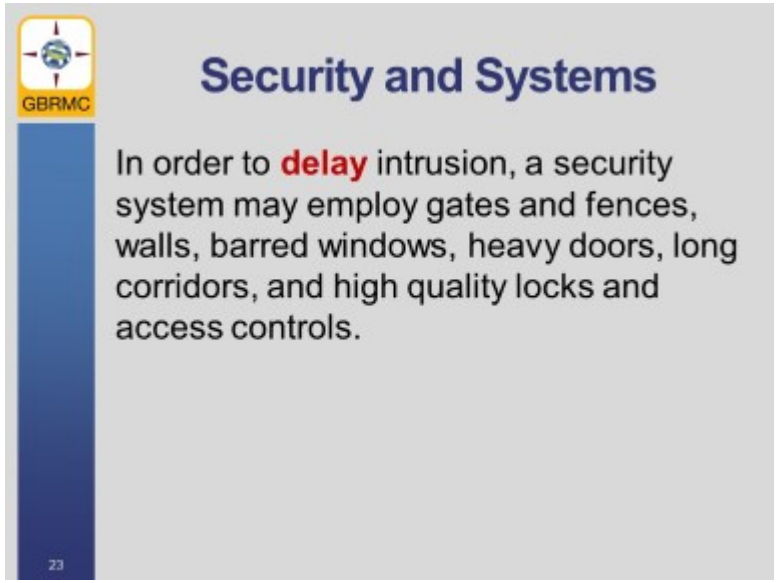

GBRMC
Design Basis Threat
One must also define what threats these assets face in order to properly secure them.
The Design Basis Threat (DBT) is the threat against which an asset must be protected and upon which the protective system's design is based
The DBT of a particular security system must be clearly articulated and documented before design and installation.
19

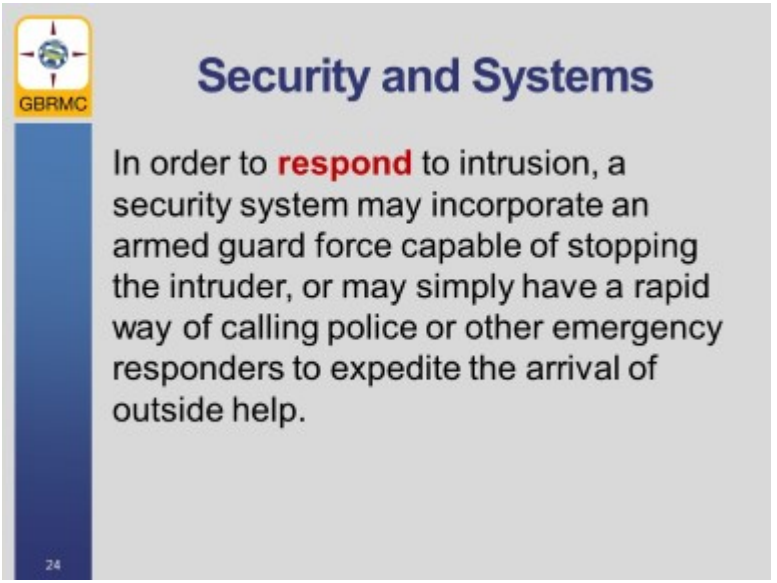

GBRMC
Design Basis Threat
One must also define what threats these assets face in order to properly secure them.
The Design Basis Threat (DBT) is the threat against which an asset must be protected and upon which the protective system's design is based
The DBT of a particular security system must be clearly articulated and documented before design and installation.
19

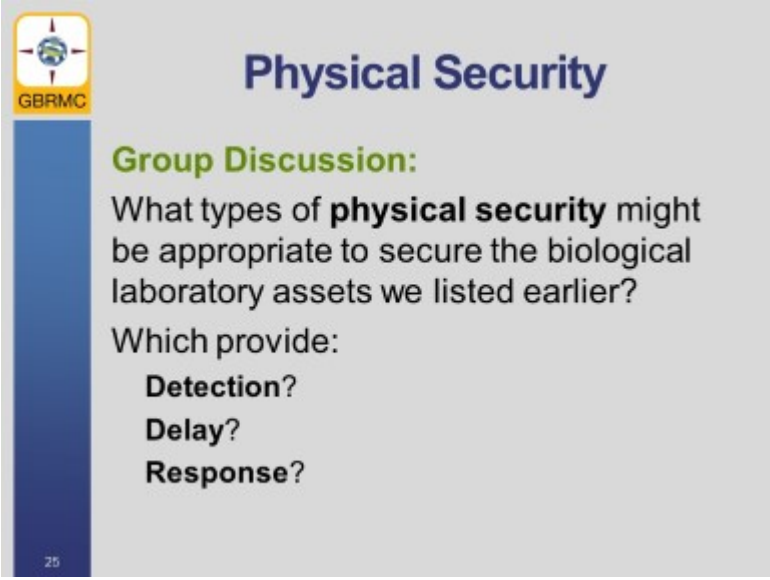

GBRMC
Security and Systems
Physical security systems are designed to:
• Detect intrusion
• Delay intrusion
• Respond to intrusion
20


GBRMC
Security and Systems
Small Group Activity:
In your groups, take 5 minutes discuss the following:
• Think about a bank. What security features typically found in a bank would you say fall under Detection, Delay, and Response?
Write your answers in your workbook.
21


GBRMC
Security and Systems
In order to detect intrusion, a physical security system may utilize sensors to determine the presence of unauthorized persons in particular areas.
These "sensors" could be as simple as a laboratorial or guard's eyes and ears, cameras and microphones, laser trip wires, heat sensors, or magnetic balance switches on doors, to name a few.
22


GBRMC
Security and Systems
In order to delay intrusion, a security system may employ gates and fences, walls, barred windows, heavy doors, long corridors, and high quality locks and access controls.
23

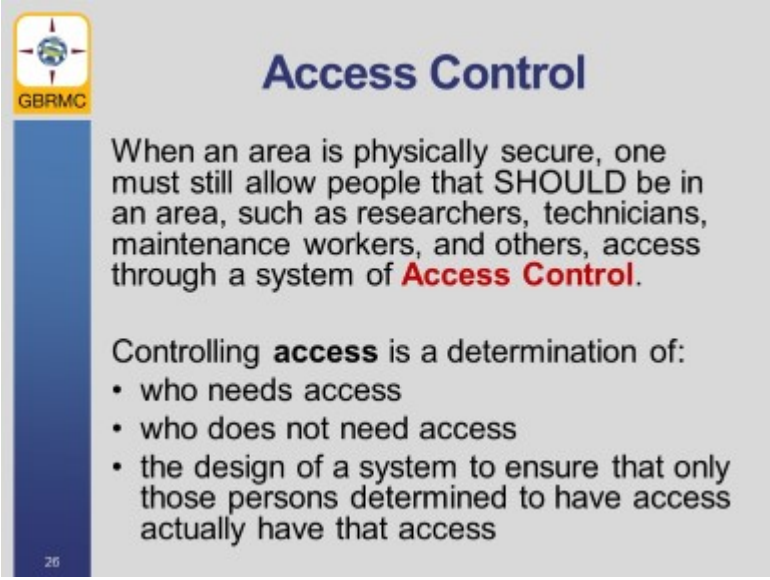

GBRMC
Security and Systems
In order to respond to intrusion, a security system may incorporate an armed guard force capable of stopping the intruder, or may simply have a rapid way of calling police or other emergency responders to expedite the arrival of outside help.
24



Detection?

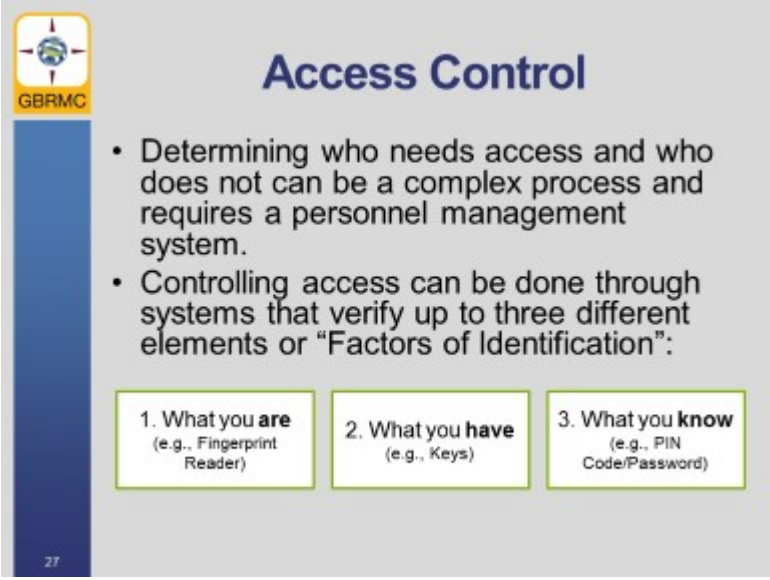
Delay?

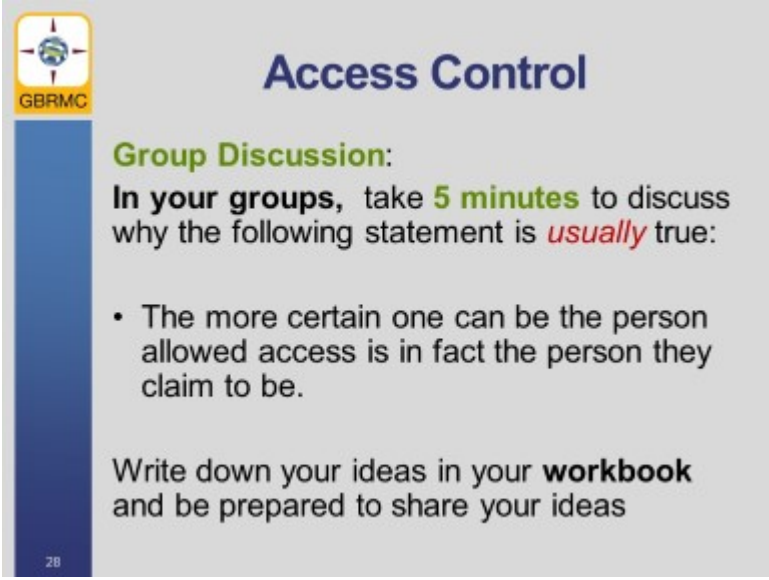
Response?



Physical security measures must always be balanced with access control.

Note: Another course detailing the management of access controls is available in the GBRMC library.


GBRMC
Access Control
• Determining who needs access and who does not can be a complex process and requires a personnel management system.
• Controlling access can be done through systems that verify up to three different elements or "Factors of Identification":
1. What you **are** (e.g., Fingerprint Reader)
2. What you **have** (e.g., Keys)
3. What you **know** (e.g., PIN Code/Password)
27


GBRMC
Access Control
Group Discussion:
In your groups, take 5 minutes to discuss why the following statement is *usually* true:
• The more certain one can be the person allowed access is in fact the person they claim to be.
Write down your ideas in your **workbook** and be prepared to share your ideas
28

GBRMC

Graded Security

Security systems can be designed and implemented to provide varying levels of protection depending on the risks assessed in particular areas. This is the concept of **graded security**.

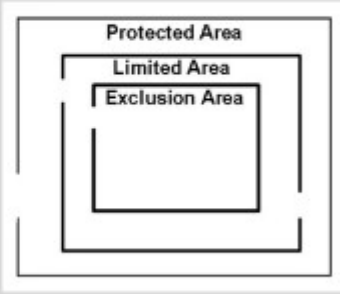
- The highest level of protection can be reserved for the most sensitive items at highest risk
- The lowest level of protection can be implemented for the least sensitive assets at lowest risk

29

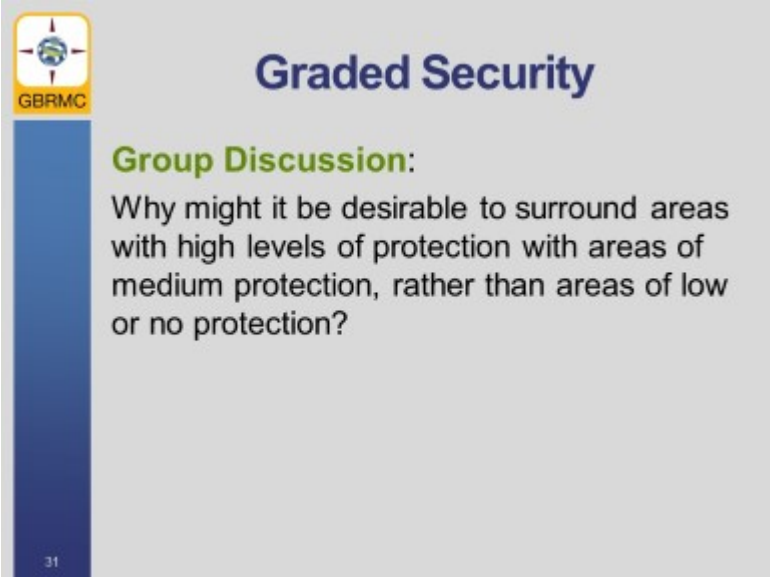
GBRMC

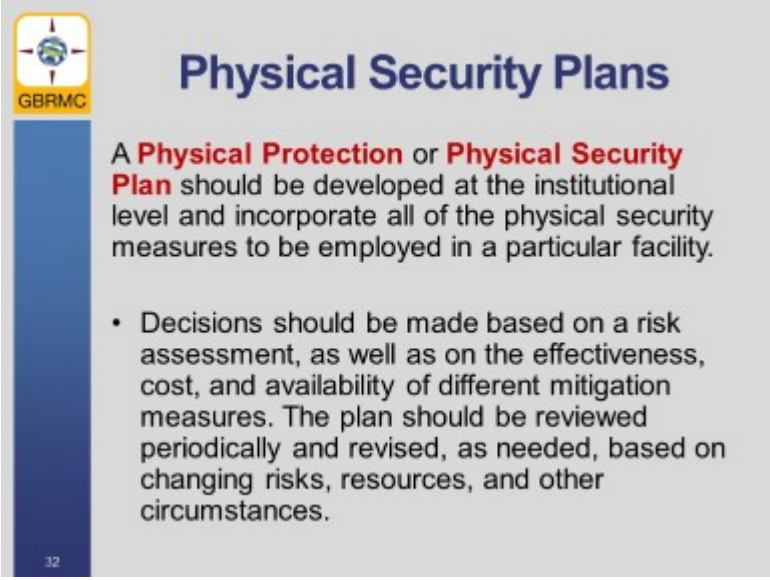
Graded Security

Graded Security can be visualized as concentric rings of security moving inward from least protected to most protected.

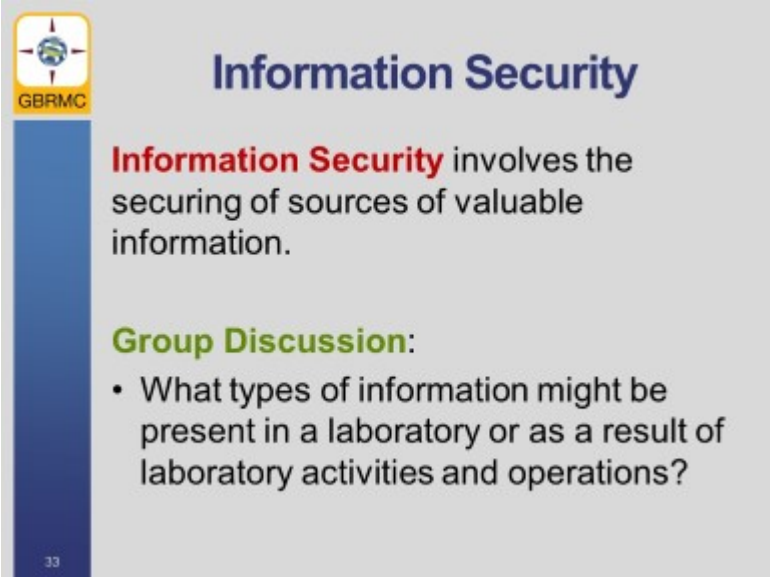


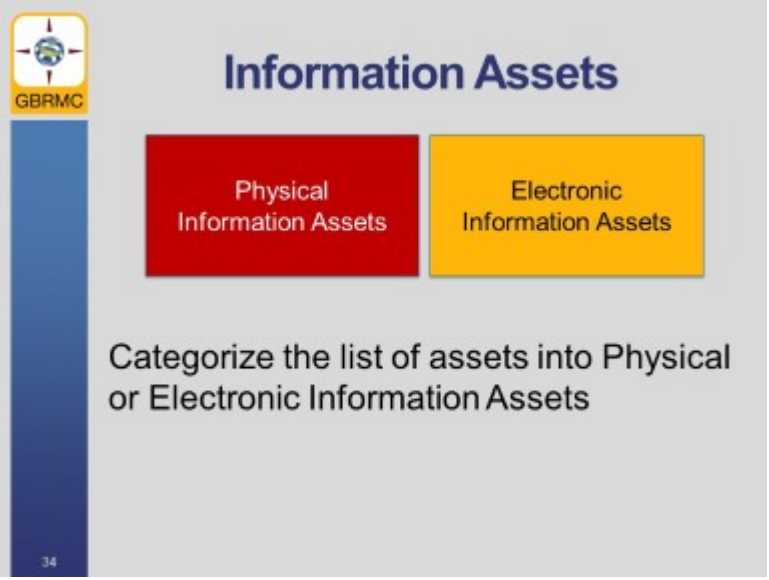
30

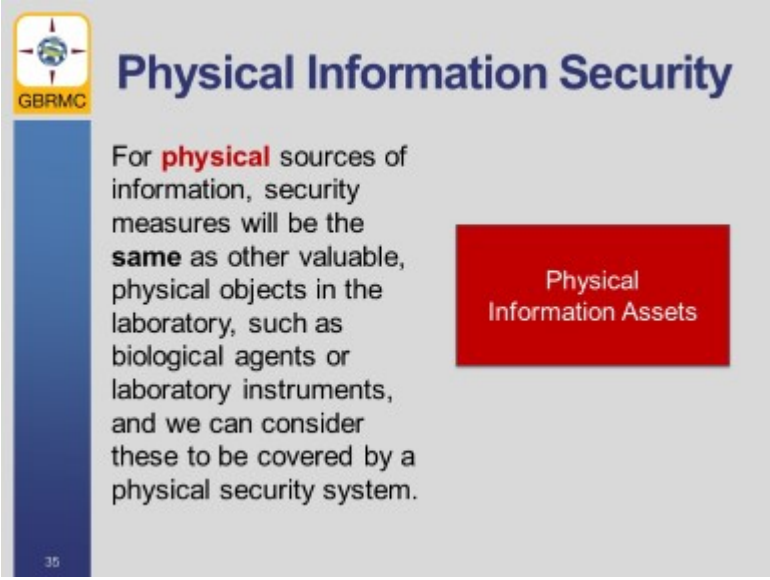

GBRMC
Graded Security
Group Discussion:
Why might it be desirable to surround areas with high levels of protection with areas of medium protection, rather than areas of low or no protection?
31



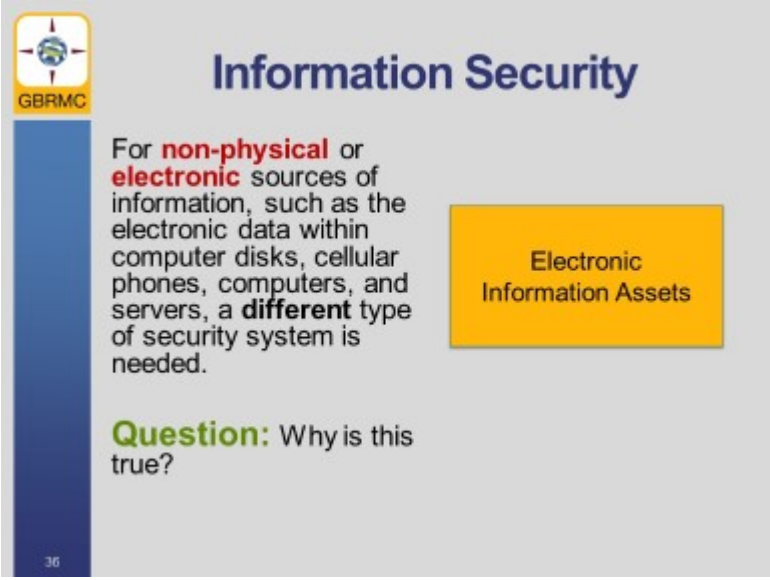
TRUE or FALSE: A Physical Security Plan needs to be updated once every five (5) years.


GBRMC
Information Security
Information Security involves the securing of sources of valuable information.
Group Discussion:
• What types of information might be present in a laboratory or as a result of laboratory activities and operations?
33

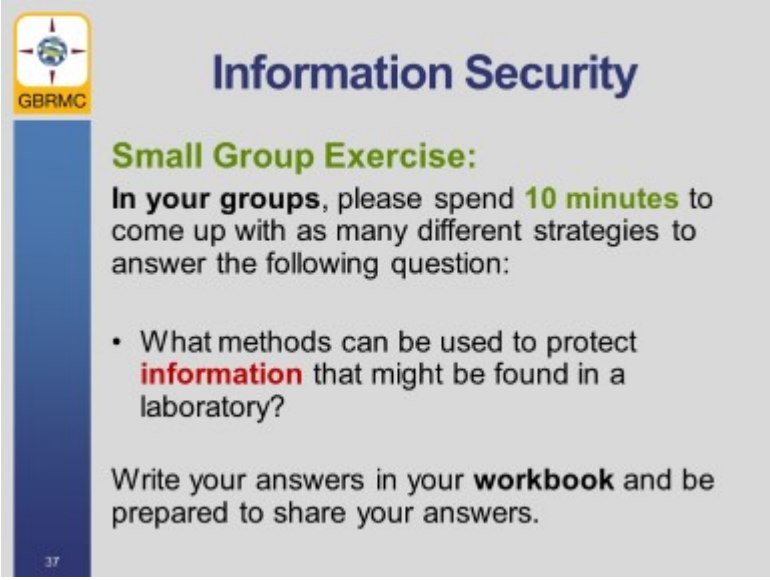

GBRMC
Information Assets
Physical Information Assets
Electronic Information Assets
Categorize the list of assets into Physical or Electronic Information Assets
34

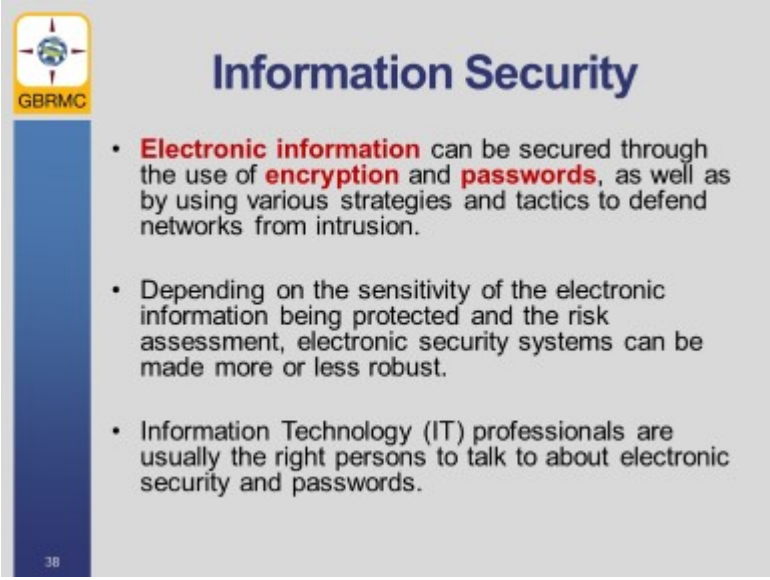


What types of physical information security sources exist in a biosciences laboratory?

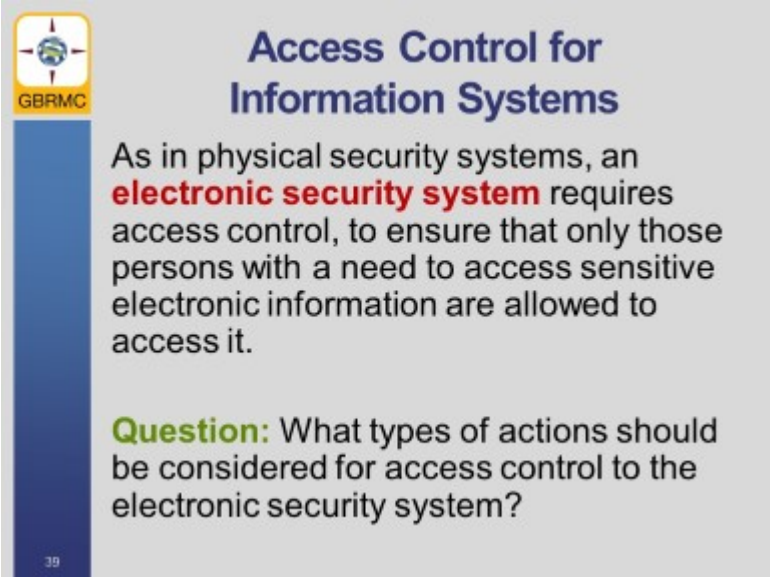


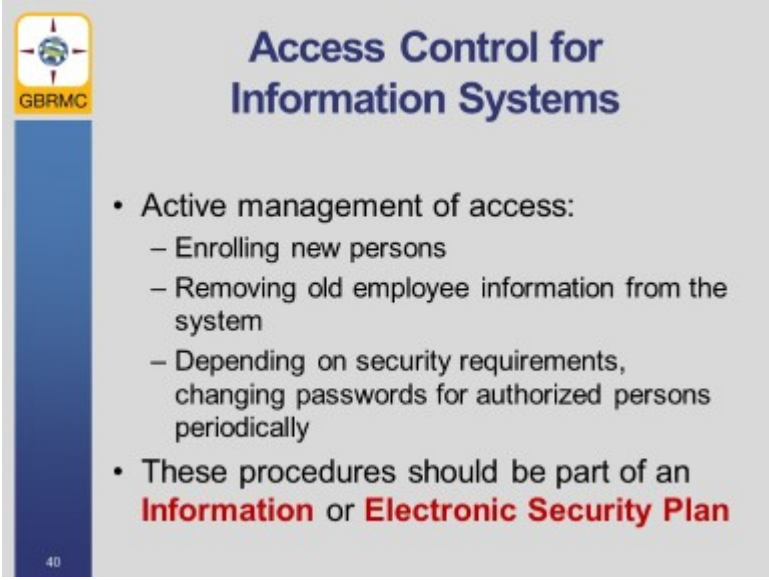
What kind of electronic sources of information exist in association with bioscience laboratories?

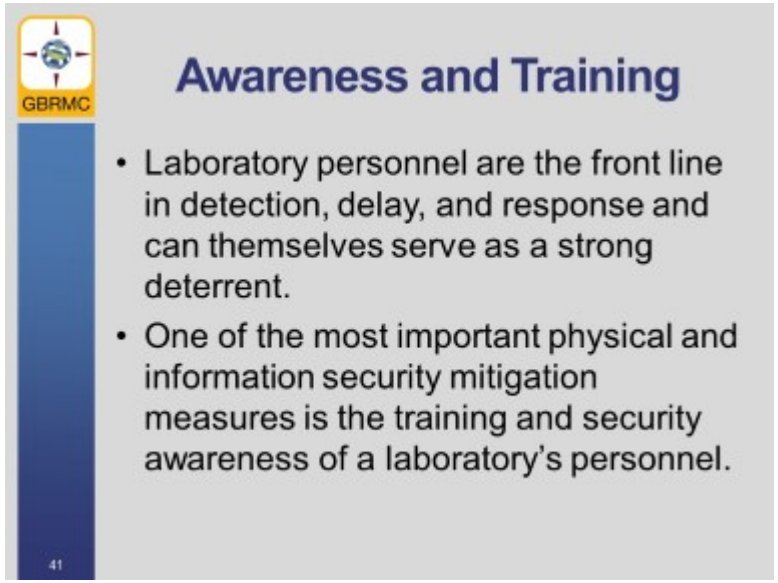

GBRMC
Information Security
Small Group Exercise:
In your groups, please spend 10 minutes to come up with as many different strategies to answer the following question:
• What methods can be used to protect information that might be found in a laboratory?
Write your answers in your workbook and be prepared to share your answers.
37

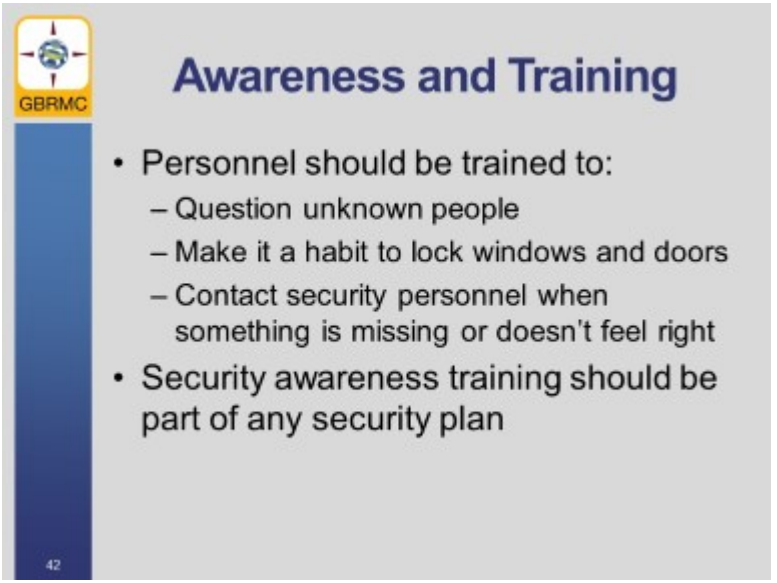


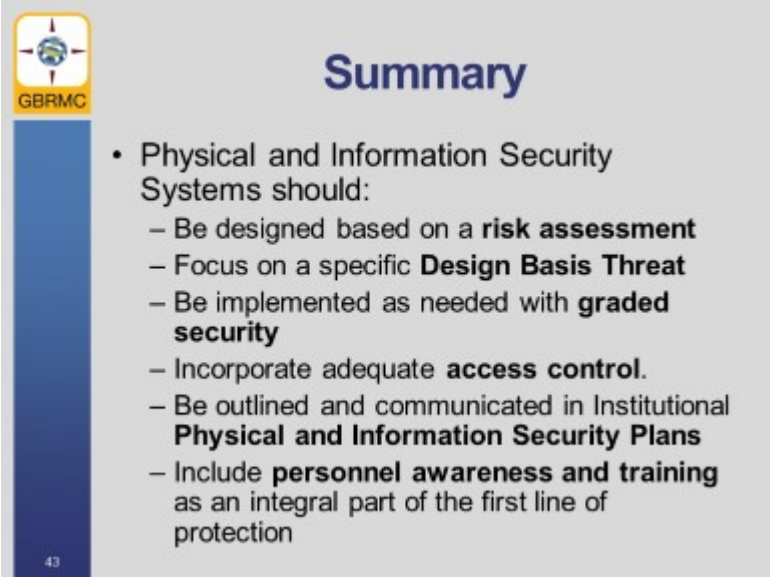
What are some methods for securing electronic information?

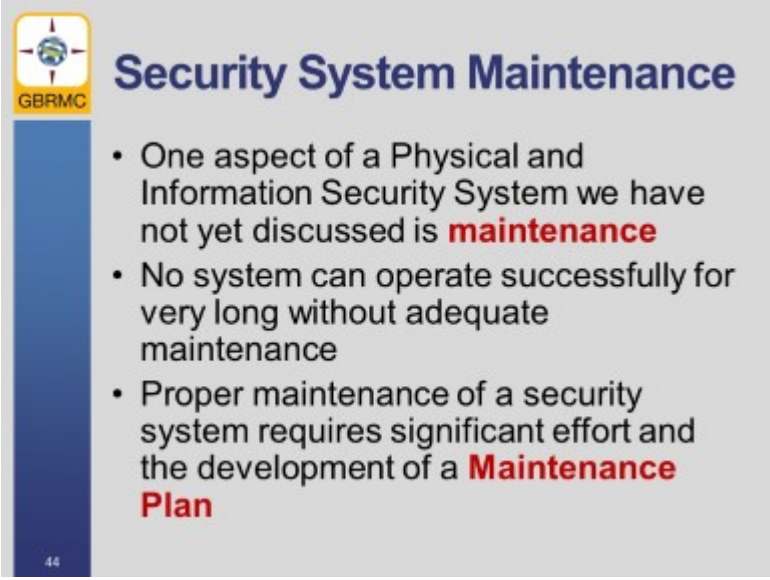

GBRMC
Access Control for Information Systems
As in physical security systems, an electronic security system requires access control, to ensure that only those persons with a need to access sensitive electronic information are allowed to access it.
Question: What types of actions should be considered for access control to the electronic security system?
39


GBRMC
Access Control for Information Systems
• Active management of access:
– Enrolling new persons
– Removing old employee information from the system
– Depending on security requirements, changing passwords for authorized persons periodically
• These procedures should be part of an Information or Electronic Security Plan
40


GBRMC
Awareness and Training
• Laboratory personnel are the front line in detection, delay, and response and can themselves serve as a strong deterrent.
• One of the most important physical and information security mitigation measures is the training and security awareness of a laboratory's personnel.
41


GBRMC
Awareness and Training
• Personnel should be trained to:
– Question unknown people
– Make it a habit to lock windows and doors
– Contact security personnel when something is missing or doesn't feel right
• Security awareness training should be part of any security plan
42


GBRMC
Summary
• Physical and Information Security Systems should:
– Be designed based on a **risk assessment**
– Focus on a specific **Design Basis Threat**
– Be implemented as needed with **graded security**
– Incorporate adequate **access control**.
– Be outlined and communicated in Institutional **Physical and Information Security Plans**
– Include **personnel awareness and training** as an integral part of the first line of protection
43



Think of an example where a security measure failed (or might fail) due to lack of maintenance.

What does effective maintenance require?

What is an example of a functionality test for a physical security system?

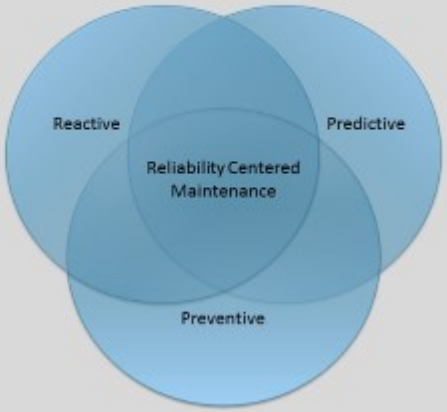
Maintenance Strategies

- **Security System Maintenance Plans** should consider different maintenance strategies:
  - Reactive Maintenance
  - Preventive Maintenance
  - Predictive Maintenance

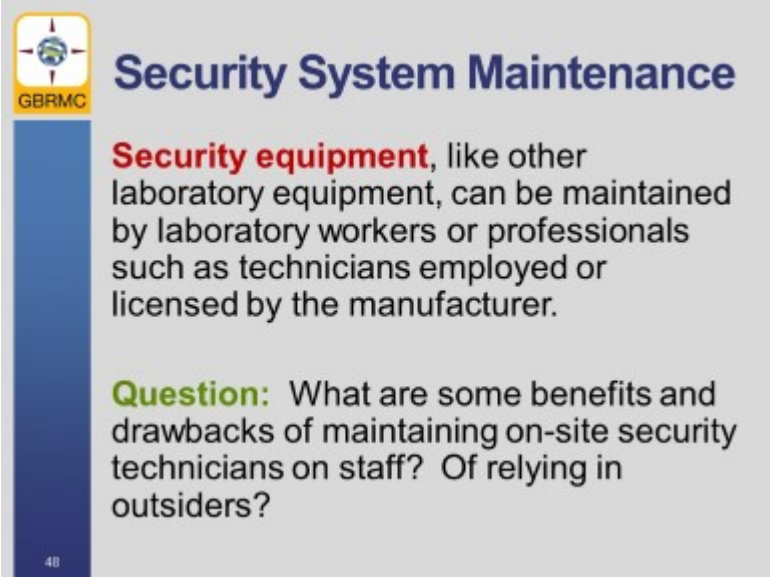
What are the differences?

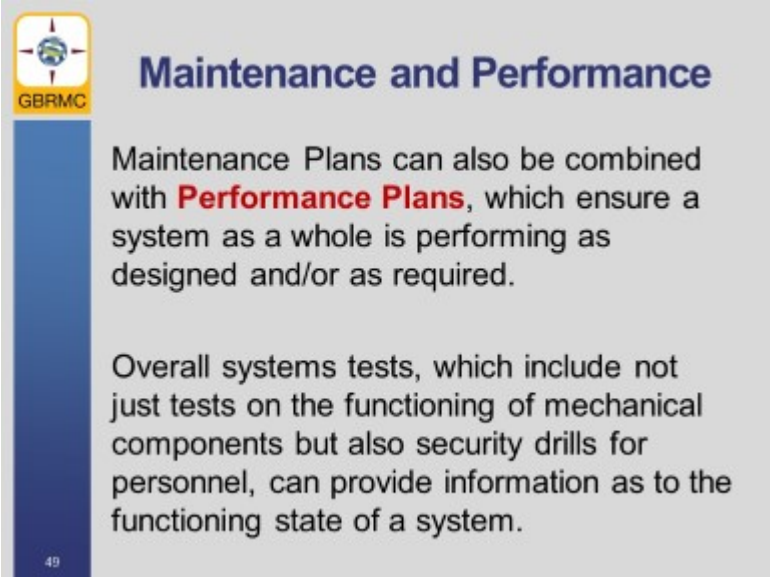
46

Reliability Centered Maintenance



47

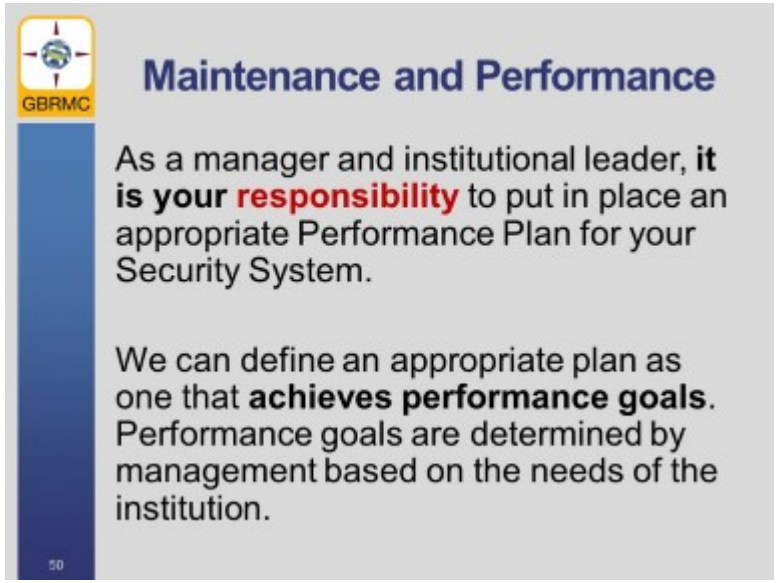

GBRMC
Security System Maintenance
Security equipment, like other laboratory equipment, can be maintained by laboratory workers or professionals such as technicians employed or licensed by the manufacturer.
Question: What are some benefits and drawbacks of maintaining on-site security technicians on staff? Of relying in outsiders?
48

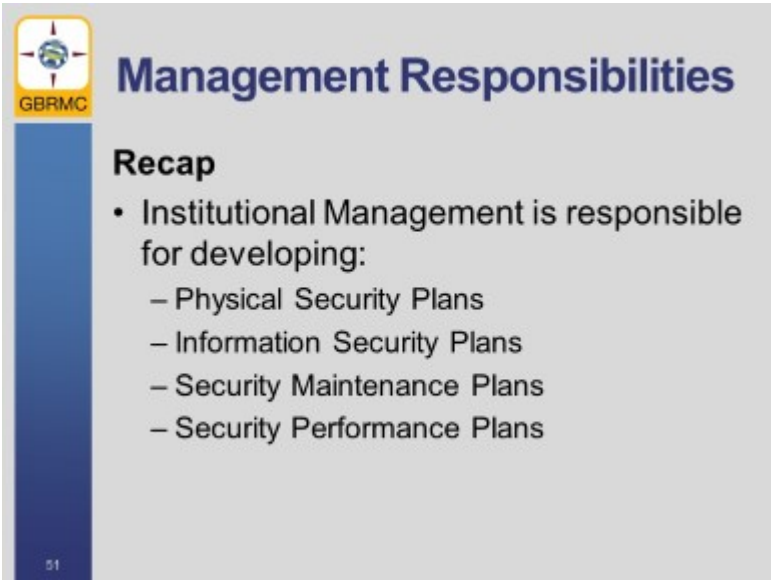


What is the difference between a Maintenance Plan and a Performance Plan?

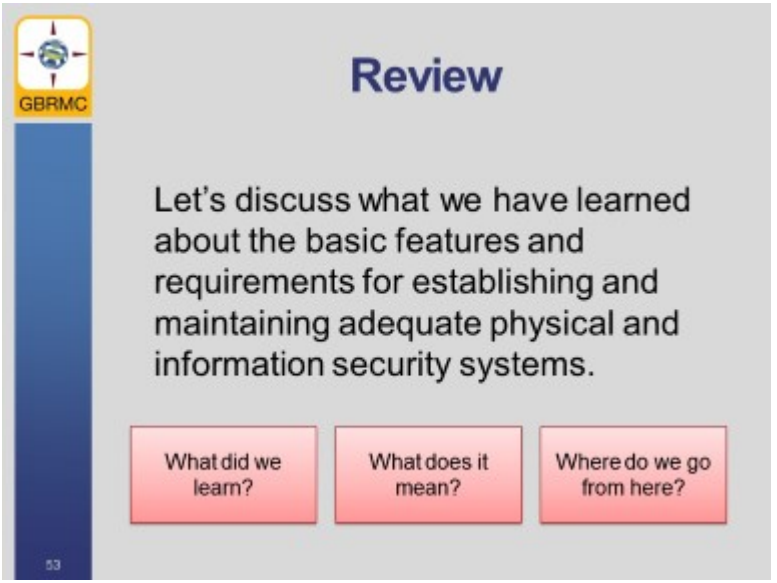
Maintenance Plan:

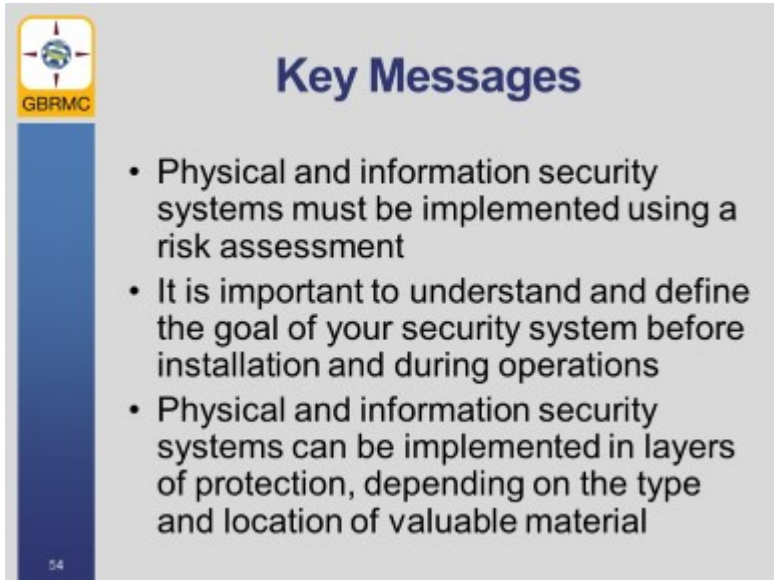
Performance Plan:

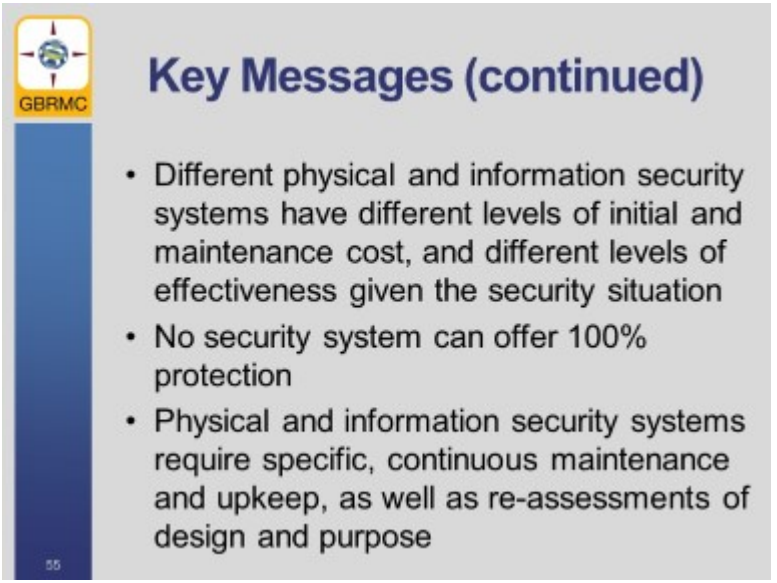

GBRMC
Maintenance and Performance
As a manager and institutional leader, it is your responsibility to put in place an appropriate Performance Plan for your Security System.
We can define an appropriate plan as one that achieves performance goals. Performance goals are determined by management based on the needs of the institution.
50


GBRMC
Management Responsibilities
Recap
• Institutional Management is responsible for developing:
– Physical Security Plans
– Information Security Plans
– Security Maintenance Plans
– Security Performance Plans
51


GBRMC
Management
• These plans can be developed independently or as part of the same master security plan
• The Security Plan itself is an integral part of a larger Institutional Biorisk Management Plan
52


GBRMC
Review
Let's discuss what we have learned about the basic features and requirements for establishing and maintaining adequate physical and information security systems.
What did we learn?
What does it mean?
Where do we go from here?
53


GBRMC
Key Messages
• Physical and information security systems must be implemented using a risk assessment
• It is important to understand and define the goal of your security system before installation and during operations
• Physical and information security systems can be implemented in layers of protection, depending on the type and location of valuable material
54


GBRMC
Key Messages (continued)
• Different physical and information security systems have different levels of initial and maintenance cost, and different levels of effectiveness given the security situation
• No security system can offer 100% protection
• Physical and information security systems require specific, continuous maintenance and upkeep, as well as re-assessments of design and purpose
55

Action Plan

By the end of this lesson, I would like to:					
KNOW		FEEL		BE ABLE TO DO	

Your learning doesn't stop with this lesson. Use this space to think about what else you need to do or learn to put the information from this lesson into practice.

What more do I need to know or do?	How will I acquire the knowledge or skills?	How will I know that I've succeeded?	How will I use this new learning in my job?