



Basic Features & Maintenance for Physical and Information Security Measures

Student Guide

2017



GLOBAL BIORISK MANAGEMENT CURRICULUM



Action Plan

By the end of this lesson, I would like to:

KNOW		FEEL		BE ABLE TO DO	
<i>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.</i>					
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?



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



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



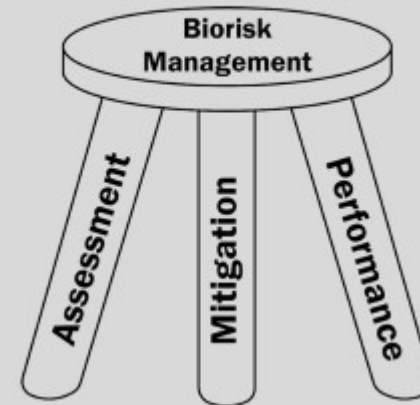
Key Messages (continued)

- 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



Biorisk Management: The AMP Model



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




Key Components of Biorisk Management

- **Biorisk Performance**
 - Improving biorisk management by recording, measuring, and evaluating organizational actions and outcomes to reduce biorisk.



10



Reasons for Physical and Info Security

Group Exercise:
In your groups, take **10 minutes** to answer the following question:

- What are some important reasons for **physical and information security** in biological laboratories?


Write your ideas on a **sticky note**. Place them on a wall or **flip chart**.

11

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

Physical security:

Information security:



Physical and Info Security

What is **physical** and **information security**?

- It is the protection of physical and informational assets in a defined space from theft, diversion, sabotage, or unauthorized access.

What are **assets**?


- What should be protected from theft, diversion, sabotage, or unauthorized access in a laboratory?

12

What is physical security?

What is information security?

What are “assets” when thinking about security issues?



Laboratory Assets

In a laboratory, **assets** could be:

- Biological Agents (Physical)
- Animals (Physical)
- Instruments and Equipment (Physical)
- Experimental Results (Information)
- Security Plans (Information)
- Employee Data (Information)
- Personnel/Staff
- Other...

While designing a security system, one must clearly define which assets one is trying to protect.

13

Other assets?



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**.



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.



Risk Assessment

Security systems must also be based on a proper **Risk Assessment**.

- What is the **likelihood** of a particular threat materializing against a particular asset?
- What are the **consequences**?


$$\text{Risk} = f(\text{Likelihood, Consequences})$$

16

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.

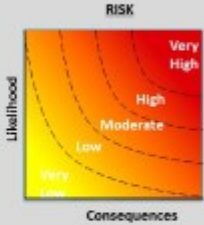
Why is a risk assessment essential to designing and implementing a security system?

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



Biosecurity Risk Assessment

A **risk assessment** assigns values for **likelihood** and **consequences**, which allows us to represent the risk of a particular adverse event on a graph.



In **Biosecurity Risk Assessment**, we are concerned with **intentional adverse events** involving laboratory disease agents, their products, and other laboratory assets.

17

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.



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



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



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



Security and Systems

Physical security systems are designed to:

- **Detect** intrusion
- **Delay** intrusion
- **Respond** to intrusion

20



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



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



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



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



Physical Security

Group Discussion:

What types of **physical security** might be appropriate to secure the biological laboratory assets we listed earlier?

Which provide:

Detection?

Delay?

Response?

25

Detection?

Delay?

Response?



Access Control

When an area is physically secure, one must still allow people that **SHOULD** be in an area, such as researchers, technicians, maintenance workers, and others, access through a system of **Access Control**.


Controlling **access** is a determination of:

- who needs access
- who does not need access
- the design of a system to ensure that only those persons determined to have access actually have that access

26

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.




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



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



Graded Security

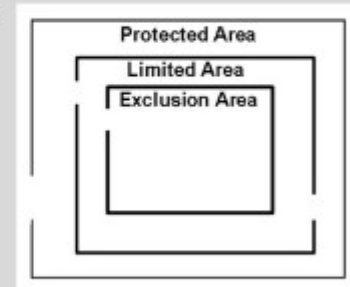
Security systems can be designed and implemented to provide varying levels of protection depending on the risks assessed in particular areas. This is the concept of **graded security**.

- 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



Graded Security

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






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




Physical Security Plans

A **Physical Protection** or **Physical Security Plan** should be developed at the institutional level and incorporate all of the physical security measures to be employed in a particular facility.

- Decisions should be made based on a risk assessment, as well as on the effectiveness, cost, and availability of different mitigation measures. The plan should be reviewed periodically and revised, as needed, based on changing risks, resources, and other circumstances.

32

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




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




Information Assets

Physical Information Assets	Electronic Information Assets
-----------------------------	-------------------------------


Categorize the list of assets into Physical or Electronic Information Assets

34




Physical Information Security

For **physical** sources of information, security measures will be the **same** as other valuable, physical objects in the laboratory, such as biological agents or laboratory instruments, and we can consider these to be covered by a physical security system.



35

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



Information Security

For **non-physical** or **electronic** sources of information, such as the electronic data within computer disks, cellular phones, computers, and servers, a **different** type of security system is needed.

Electronic Information Assets

Question: Why is this true?

36

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



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



Information Security

- **Electronic information** can be secured through the use of **encryption** and **passwords**, as well as by using various strategies and tactics to defend networks from intrusion.
- Depending on the sensitivity of the electronic information being protected and the risk assessment, electronic security systems can be made more or less robust.
- Information Technology (IT) professionals are usually the right persons to talk to about electronic security and passwords.

38

What are some methods for securing electronic information?



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



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



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



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



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




Security System Maintenance

- One aspect of a Physical and Information Security System we have not yet discussed is **maintenance**
- No system can operate successfully for very long without adequate maintenance
- Proper maintenance of a security system requires significant effort and the development of a **Maintenance Plan**

44

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

What does effective maintenance require?



Security System Maintenance

- **Security System Maintenance Plans** should:
 - compile all technical maintenance requirements from equipment manufacturers
 - include schedules for regular tests to ensure system components remain functional
- Plans should also provide a listing of the means to repair or replace components in the event they are not functioning properly

45

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



Maintenance Strategies

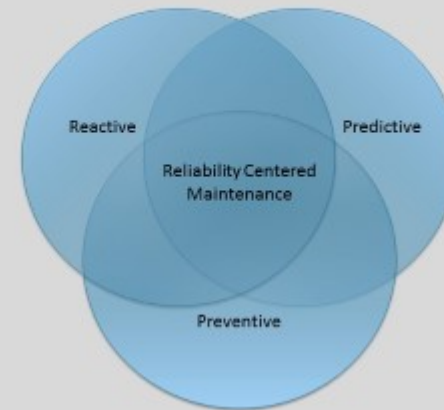
- **Security System Maintenance Plans** should consider different maintenance strategies:
 - Reactive Maintenance
 - Preventive Maintenance
 - Predictive Maintenance

What are the differences?

46



Reliability Centered Maintenance



47



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



Maintenance and Performance

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

Overall systems tests, which include not just tests on the functioning of mechanical components but also security drills for personnel, can provide information as to the functioning state of a system.

49

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

Maintenance Plan:

Performance Plan:



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



Management Responsibilities

Recap

- Institutional Management is responsible for developing:
 - Physical Security Plans
 - Information Security Plans
 - Security Maintenance Plans
 - Security Performance Plans

51



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



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



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



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?