

Welcome to the Data Protection Module. Here, we will explore how to protect data effectively.

Data Protection is important because it ensures the privacy and security of sensitive information, prevents unauthorized access, and builds trust with users and stakeholders.

Select all the data that you think needs to be protected.

- personal information
- financial records
- medical records
- business secrets
- login credentials
- any other sensitive data.

That's Correct! Data privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). This includes financial information, medical records, social security or ID numbers, names, birthdates, and contact information.

Oh no! We have identified a data breach. Let's look into this further

A data breach is a security incident where unauthorized parties access sensitive or confidential information.

Three scenarios will be shown. Identify whether a breach could have occurred.

Here the user will be able to see failed login attempts in an Oracle Database

Yes No

A scene showing Unknown Devices Connected to the network

Yes No

A scene showing an increased number or suspicious emails

Yes No

Select all the ways to prevent a data breach


- Use strong and unique passwords.
- Enable multi-factor authentication (MFA).
- Regularly update and patch software.
- Encrypt sensitive data.
- Conduct employee cybersecurity training.

That's Correct. Organizations and employees must implement and follow best practices that support a data breach prevention plan. These include strong password, multi-factor authentication, update software regularly and create a response plan


Now let's learn how to protect a shared folder. Follow the steps below and learn how to set up secure access permissions and encryption for a shared document repository

You have successfully completed the Data Protection Module!!

Create your own at Storyboard That



**Welcome to the Data
Protection Module. Here, we
will explore how to protect
data effectively.**



Data Protection is important because it ensures the privacy and security of sensitive information, prevents unauthorized access, and builds trust with users and stakeholders.

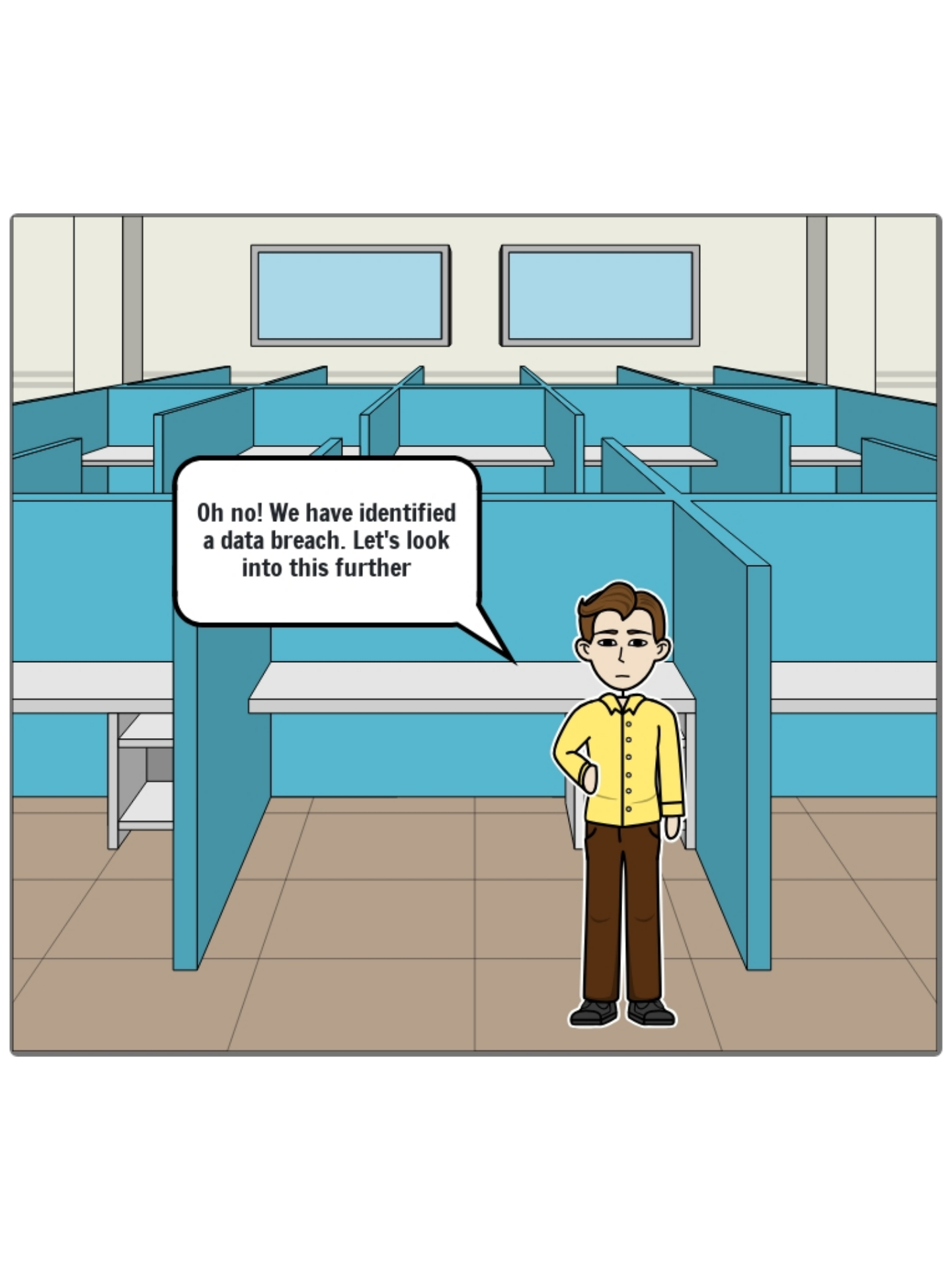
Select all the data that you think needs
to be protected:

- ☐ • personal information
- ☐ • financial records
- ☐ • medical records
- ☐ • business secrets
- ☐ • login credentials
- ☐ • any other sensitive data.



That's Correct!
Data privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). This includes financial information, medical records, social security or ID numbers, names, birthdates, and contact information.



A cartoon illustration of a man with brown hair, wearing a yellow button-down shirt and brown trousers, standing in the center of an empty office. The office is filled with blue cubicles that have white desks. Two empty rectangular frames hang on the light-colored wall in the background. The floor is made of large brown tiles. A speech bubble points from the man's head towards the left.

**Oh no! We have identified
a data breach. Let's look
into this further**

An illustration of an office environment with several cubicles. A man with brown hair, wearing a yellow button-down shirt and brown trousers, stands in the foreground. He is pointing his right hand towards a speech bubble that contains text. The office has blue cubicle walls, white desks, and a brown tiled floor. Two empty rectangular frames are mounted on the back wall.

A data breach is a security incident where unauthorized parties access sensitive or confidential information.

**Three scenarios will be shown.
Identify whether a breach could have
occurred.**



**Here the user will be able to see failed login attempts
in an Oracle Database**

Yes

No

A scene showing Unknown Devices Connected to the network

Yes

No

A scene showing an increased number or suspicious emails

Yes

No

Select all the ways to prevent a data breach

- ☐ • **Use strong and unique passwords.**
- ☐ • **Enable multi-factor authentication (MFA).**
- ☐ • **Regularly update and patch software.**
- ☐ • **Encrypt sensitive data.**
- ☐ • **Conduct employee cybersecurity training.**

That's Correct.

Organizations and employees must implement and follow best practices that support a data breach prevention plan. These include strong passwords, multi-factor authorization, update software regularly and create a response plan



Now let's learn how to protect a shared folder.

Follow the steps below and learn how to set up secure access permissions and encryption for a shared document repository





You have successfully completed the Data Protection Module!!