This study guide demonstrates the lesson from *The Shared Responsibility Model – What are My Responsibilities?*
My full AWS Architect Associate course can be found here:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361

AWS Shared Responsibility Model Study Guide

In this lesson, we delve into the core concept of the AWS Shared Responsibility Model. This model outlines the distribution of security responsibilities between AWS, the cloud service provider, and you, the customer, when you create an account on AWS.

1. Security of the Cloud vs. Security in the Cloud:

- AWS provides "Security of the Cloud," encompassing the physical security of data centers, secure hardware retirement, and network-level security, including border firewalls.
- As the customer, you are responsible for "Security in the Cloud." This includes tasks like patching and hardening guest operating systems, creating security groups to manage network traffic, and effectively managing Identity and Access Management (IAM) credentials. Multi-factor authentication (MFA) is also recommended to enhance security.

2. Managed Services:

- AWS takes administrative responsibility for "Managed Services," such as patching the operating system and minimizing the attack surface. However, customers retain the responsibility for user access and account management.

3. Data Destruction:

- AWS handles the secure destruction of data on decommissioned storage systems, relieving customers of this task.

4. Virtual Private Cloud (VPC):

- Customers are responsible for creating their own Virtual Private Cloud (VPC) rather than relying on the default VPC automatically provided when signing up for an AWS account. The VPC acts as an isolated environment, enabling control over resources with features like security groups and access lists.

5. Unmanaged Services:

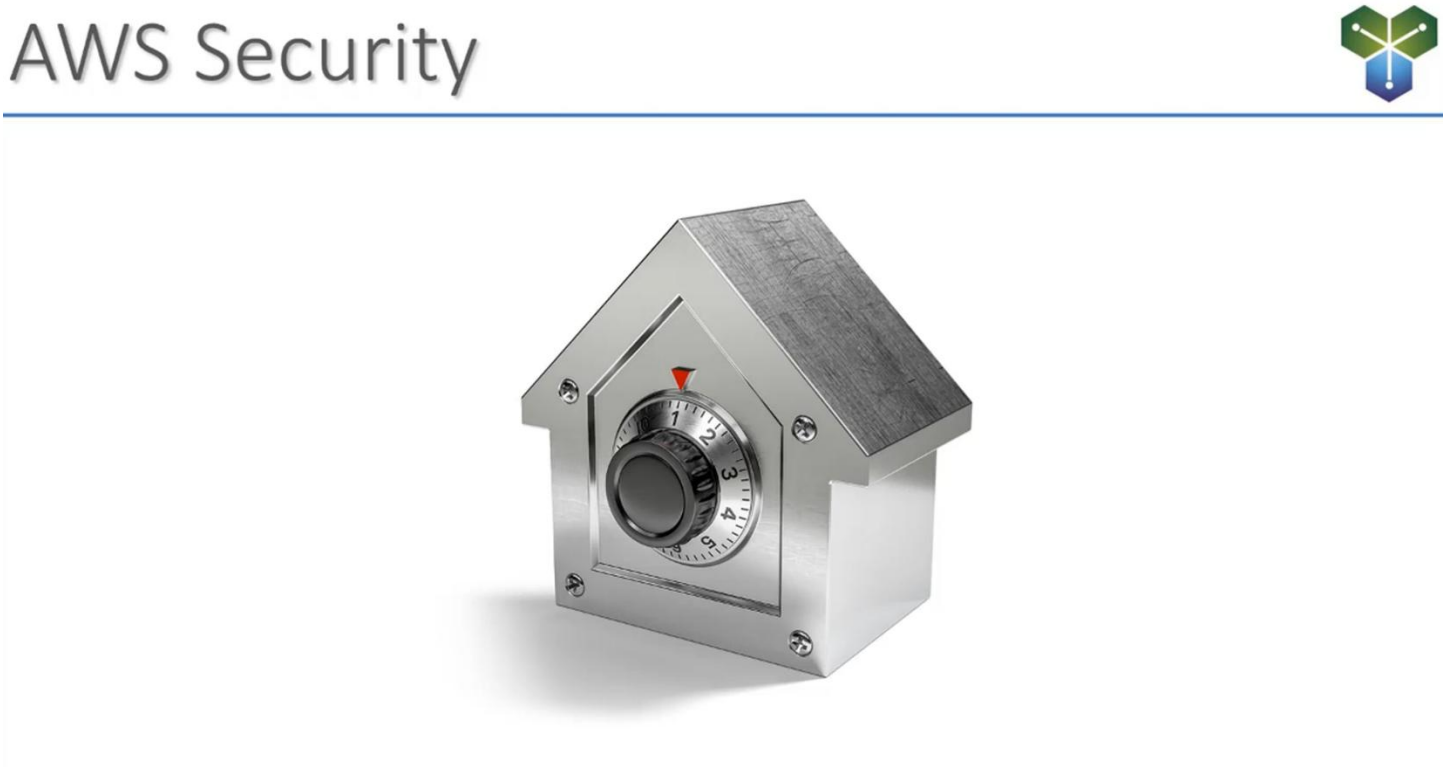
- For unmanaged services like Amazon EC2, where customers have full control over the operating system, it is your responsibility to keep the OS patched, install antivirus, and configure necessary security measures like firewalls.

6. Managed Service Security:

- Even on managed services like Amazon S3 for storage, customers must take charge of securing their content. This includes managing the public or private status of S3 buckets and configuring roles and permissions to control access to bucket contents.

Understanding the AWS Shared Responsibility Model is essential for ensuring a secure and compliant AWS environment. AWS handles certain security aspects, but it's crucial for customers to be aware of their responsibilities and actively manage them to maintain a robust security posture.

See slides below:



Shared Responsibility Model

AWS:

- Physical Security, Hardware Retirement, Border Firewall

Customer:

- Guest O.S Patching, Security Groups, IAM

Additional AWS Responsibilities

- Updates and Anti-virus on managed services
- The customer is still responsible for user access and account management
- Destruction of retired storage systems

Additional Customer Responsibilities

- VPC
- EC2 instances
- S3

For more details see my full AWS Architect Associate course:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361