Asset_Home_Network

Activity: Classify the Assets connected to a home Network

In this activity, you will classify assets connected to a home office network.
Asset management is a critical part of every organization's security plan. Remember that asset management is the process of tracking assets and the risks that affect them. Effective asset management starts with creating an asset inventory, or a catalog of assets that need to be protected. Then, it involves classifying assets based on their level of importance and sensitivity to risk.
Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then, complete the step-by-step instructions.
One of the most valuable assets in the world today is information. Most information is accessed over a network. There tend to be a variety of devices connected to a network and each is a potential entry point to

other assets.
An inventory of network devices can be a useful asset management tool. An inventory can highlight sensitive assets that require extra protection.
You're operating a small business from your home and must create an inventory of your network devices. This will help you determine which ones contain sensitive information that require extra protection.
To do this, you will start by identifying three devices that have access to your home network. This might include devices such as:
Desktop or laptop computers
Smartphones
Smart home devices
Game consoles
Storage devices or servers
Video streaming devices
Then, you'll list important characteristics of each device such as its owner, location, and type. Finally, you will assign each device a level of sensitivity based on how important it is to protect.

Step-By-Step Instructions

Follow the instructions and answer the end-of-activity question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step1: Access the template

A	B	C	D	E	F
	Asset	Network access	Owner	Location	Notes
1	Network router	Continuous	Internet service provider (ISP)	On-premises	Has a 2.4 GHz and 5 GHz connection. All devices on the home network connect to the 5 GHz frequency.
2	Desktop	Occasional	Homeowner	On-premises	Contains private information, like photos.
3	Guest Smartphone	Occasional	Friend	On and Off-premises	Connects to my home network.
4					
5					
6					

Categories	Access destination
Restricted	Need-to-know
Confidential	Limited to specific users
Internal-Only	Users on-premises
Public	Anyone

Step 2: Identify assets

In the asset inventory spreadsheet, find the Asset column header. Consider the devices that may be connected to the home network. Examine devices in the scenario graphic to help you brainstorm.

Choose three devices that are not already listed in the spreadsheet and add them to the empty rows in the Asset column.

Note: A few devices, like a network router, desktop, and a guest smartphone have already been added for your reference.

4: Laptop 5: Smart Home Hub 6: Network-Attached Storage

A	B	C	D	E	F
	Asset	Network access	Owner	Location	Notes
1	Network router	Continuous	Internet service provider (ISP)	On-premises	Has a 2.4 GHz and 5 GHz connection. All devices on the home network connect to the 5 GHz frequency.
2	Desktop	Occasional	Homeowner	On-premises	Contains private information, like photos.
3	Guest Smartphone	Occasional	Friend	On and Off-premises	Connects to my home network.
4	Laptop	Occasional	Homeowner	On-premises	Contains important work documents and is used occasionally for business-related tasks.
5	Smart Home Hub	Continuous	Homeowner	On-premises	Central hub for controlling smart home devices and continuously connected to the network.
6	Network-attached storage	Continuous	Homeowner	On-premises	Used for storing business-related data, accessible to users on-premises.

Step 3: Fill in the characteristics of each asset

List important characteristics, including Network access, Owner, and Location for each asset that you've identified.

Here's an explanation of each characteristic:

Network access describes how often the device is connected to the network.

Owner describes the person responsible for the device.

Location describes where the device is located in relation to the router.

Filled in the on yellow highlight above

Laptop (Row 4):
Network access: Occasional
Owner: Homeowner
Location: On-premises

Smart Home Hub (Row 5):
Network access: Continuous
Owner: Homeowner
Location: On-premises

Network-Attached Storage (Row 6):
Network access: Continuous

Owner: Homeowner
Location: On-premises

Step 4: Evaluate the access of network devices

Review the information that you've listed in the Network access, Owner, and Location columns.
In the Notes column, record 1 or 2 details or characteristics of each device. Do this by asking yourself questions about each:
What kind of information is stored on the device?
How does it connect to the network?
Is the owner careful about securing it?
For example, the desktop computer contains sensitive information, like photos, that only the owner should have access to. In contrast, the network router uses one frequency for smart home devices and another for all other devices.
Note: Keep in mind that there might be some variation within each category. Try to identify details that could impact the confidentiality, integrity, or availability of information that's connected to the network.
Laptop (Row 4):
Notes: Contains important work documents and is used occasionally for business-related tasks.

Smart Home Hub (Row 5):
Notes: Central hub for controlling smart home devices and continuously connected to the network.

Network-Attached Storage (Row 6):
Notes: Used for storing business-related data, accessible to users on-premises.

Step 5: Classify the sensitivity of network devices

It's time to classify assets based on the information you've collected. Do this by thinking about how an asset could impact your business if its security was compromised:
What types of information would be disclosed or stolen?
Could an attacker alter information on the device?
What would happen to the business if this information were destroyed?
For example, the network router is classified as confidential because the owner has granted limited access to the device to specific users.
Find the Sensitivity column in the asset inventory. Type one of the four levels of sensitivity you previously learned about.
Note: You can use the Categories table as a guide for choosing an appropriate classification.

Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to include the following elements in your completed activity:
List of 3 devices on the home network
List network access, owner, and location for each device
1–2 notes on network access
A sensitivity classification
Laptop (Row 4): Sensitivity: Restricted

Smart Home Hub (Row 5): Sensitivity: Confidential
Network-Attached Storage: (Row 6): Sensitivity: Confidential