CDM Hardware Asset Management (HWAM) Capability

Department of Homeland Security
Office of Cybersecurity and Communications
Federal Network Resilience

Table of Contents

1 PURPOSE AND SCOPE 2

2 THREAT / ATTACKS 3

1. QUESTION: WHAT TYPES OF ATTACKS ARE ADDRESSED WITH HARDWARE ASSET MANAGEMENT (HWAM)? 3

2. QUESTION: HOW DOES HARDWARE ASSET MANAGEMENT ADDRESS ATTACKS ON UNMANAGED SYSTEMS? 4

3. QUESTION: HOW DOES HARDWARE ASSET MANAGEMENT RELATE TO THE OTHER CDM CAPABILITIES? 5

3 INTEGRATION 5

4. QUESTION: WHAT CAPABILITIES SUPPORT HARDWARE ASSET MANAGEMENT? 5

5. QUESTION: WHAT CAPABILITIES DOES HARDWARE ASSET MANAGEMENT SUPPORT? 5

6. QUESTION: WHAT OTHER CAPABILITIES PROVIDE "COMPENSATING CONTROLS" TO HARDWARE ASSET MANAGEMENT? 5

4 DESIRED STATE 6

7. QUESTION: WHAT IS A DEVICE? 6

8. QUESTION: WHEN IS A DEVICE CONSIDERED AUTHORIZED? 6

9. QUESTION: WHAT IS THE HARDWARE ASSET MANAGEMENT DESIRED STATE? 6

10. QUESTION: WHAT DATA SHOULD BE RECORDED IN THE HARDWARE ASSET MANAGEMENT DESIRED STATE INVENTORY? 7

11. QUESTION: HOW CAN AN ORGANIZATION DETERMINE ITS DESIRED STATE? 8

12. QUESTION: HOW SHOULD/COULD AN ORGANIZATION ASSIGN MANAGERS FOR HARDWARE ASSET MANAGEMENT ASSETS? 9

13. QUESTION: CAN I SIMPLY USE MY PROPERTY MANAGEMENT SYSTEM AS DESIRED STATE? 10

14. QUESTION: IS NAC A GOOD SOLUTION FOR ACHIEVING HARDWARE ASSET MANAGEMENT? 11

5 ACTUAL STATE 11

15. QUESTION: WHAT IS THE HARDWARE ASSET MANAGEMENT "ACTUAL STATE"? 11

16. QUESTION: HOW DOES AN ORGANIZATION DETERMINE ITS HARDWARE ASSET MANAGEMENT ACTUAL STATE? 12

17. QUESTION: WHAT DATA SHOULD BE RECORDED IN THE HARDWARE ASSET MANAGEMENT ACTUAL STATE INVENTORY? 12

6 FINDING RISK CONDITIONS AND DEFECTS 13

18. QUESTION: HOW DOES AN ORGANIZATION FIND THE DIFFERENCE BETWEEN DESIRED STATE AND ACTUAL STATE IN HARDWARE ASSET MANAGEMENT? 13

19. QUESTION: WHY IS THE GAP BETWEEN DESIRED STATE AND ACTUAL STATE IMPORTANT? 14

7 FIXING DEFECTS 15

20. QUESTION: HOW CAN AN ORGANIZATION ADDRESS THE DIFFERENCE BETWEEN ACTUAL AND DESIRED STATE? 15

21. QUESTION: HOW CAN WE PREVENT UNAUTHORIZED DEVICES FROM GETTING ON THE NETWORK IN THE FIRST PLACE? 16

1 PURPOSE AND SCOPE

This toolkit outlines and documents issues of relevance to implementing the Hardware Asset Management (HWAM) Capability as part of Continuous Diagnostics and Mitigation (CDM). This toolkit provides general information on the HWAM capabilities and implications thereof. Further, this toolkit highlights considerations that technical implementers as well as managers may have when understanding how to effectively implement HWAM to better manage cybersecurity risk.

Additional considerations, inquiries, and suggestions for revision or addition can be submitted to: cdm.fnr@hq.dhs.gov. This toolkit will be updated as required.

2 THREAT / ATTACKS

1. QUESTION: WHAT TYPES OF ATTACKS ARE ADDRESSED WITH HARDWARE ASSET MANAGEMENT (HWAM)?

Answer: HWAM addresses attacks on vulnerable machines—new and unprotected systems as well as "forgotten" machines.

Background: Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them; exploiting these machines allows attackers to gain a foothold on the network. Attackers also exploit forgotten machines that no one is managing; these machines are particularly vulnerable to attacks due to outdated patches and configurations. Incident reports reveal that unmanaged machines play a significant role in high-impact attacks and exploitations of networks.

Definition: In this context, a *system* is a machine (device) that can be exploited remotely, over the network, or through physical access.

*The Hardware Asset Management capability addresses whether someone is assigned to manage the machine and whether the machine is authorized. It does not address how **well** the machine is managed. Quality of management is covered by Software Asset Management (SWAM), Configuration Setting Management (CSM), and Vulnerability Management (VUL).*

One reason unmanaged devices are more vulnerable is that no one is actively managing software installation, configuration settings, and vulnerabilities. This leaves the software on those devices with a higher risk of successful attack.

If we don't know who is managing the device,

- *We can't send the responsible individual(s) data to identify problems with software installed (SWAM), configuration settings (CSM), and patching (VUL).*
- *We can't hold anyone responsible for poor management of the device.*

2. QUESTION: HOW DOES HARDWARE ASSET MANAGEMENT ADDRESS ATTACKS ON UNMANAGED SYSTEMS?

Answer: This capability addresses attacks on unmanaged systems by reducing the number of such machines on the network.

After quickly identifying an unmanaged machine, the methods below can reduce cybersecurity risk:

Primary Methods

- Quickly remove the unmanaged machine from the network
- Quickly assign the unmanaged machine to be managed by a specific group

Preventative Methods

- Develop processes to prevent new unmanaged machines from appearing on the network
- Develop processes to prevent previously managed machines from becoming unmanaged (This typically happens when a device manager leaves the organization, and devices are not re-assigned.)

Background: Though NIST interprets SP 800-53 as requiring hardware inventory control, few agencies (as of 2013) manage their hardware inventory in a way that eliminates unmanaged machines; US-CERT frequently finds attacks on unmanaged machines.

A vulnerable condition is required for a successful attack on unmanaged hardware. Unmanaged hardware assets are more likely to be vulnerable to attacks; successful attacks on these assets often go undetected because no one is attending to them.

Links to Related Resources
NIST Guidance:
• NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf]
DHS/FNR CDM Guidance:
• List of 800-53 controls that support implementation of the Hardware Asset Management capability [http://en.wikipedia.org/wiki/NIST_Special_Publication_800-53]

3. QUESTION: HOW DOES HARDWARE ASSET MANAGEMENT RELATE TO THE OTHER CDM CAPABILITIES?

Answer: The Hardware Asset Management (HWAM) capability:

- is one of four capabilities that focus on device management
  The other device management capabilities are
  - Software Inventory Management (SWAM)
  - Configuration Setting Management (CSM)
  - Vulnerability (Patch) Management (VUL)
- is the first step in identifying the installed software (SWAM), and knowing whether it has safe settings (CSM) and patches (VUL). Hardware Asset Management is foundational to SWAM, CSM, and VUL.
  - If you don't know you have the hardware, you can't check these other items.
  - If you don't know you have the hardware, you won't assign it for management.

3 INTEGRATION

4. QUESTION: WHAT CDM CAPABILITIES SUPPORT HARDWARE ASSET MANAGEMENT?

Answer: None. HWAM is the first step in CDM and supports all other capabilities.

5. QUESTION: WHAT CAPABILITIES DOES HARDWARE ASSET MANAGEMENT SUPPORT?

Answer: HWAM supports SWAM, CSM, and VUL. Since HWAM is the first step in proper execution of CDM, HWAM must be implemented before the other capabilities can be executed. For example, it is impossible to determine which vulnerabilities exist in software if an organization doesn’t know what software is installed, and it is impossible to manage installed software without knowing which devices exist to install the software upon.

6. QUESTION: WHAT OTHER CAPABILITIES PROVIDE “COMPENSATING CONTROLS” TO HARDWARE ASSET MANAGEMENT?

Answer: In certain special circumstances, CSM can provide compensating controls to HWAM (for example, where the settings exist to discover new devices on a network).

4 DESIRED STATE

7. QUESTION: WHAT IS A DEVICE?

Answer: For the purposes of Hardware Asset Management, a device is:

- Any hardware asset that is addressable (i.e., has an IP address) and is connected to your organization's network(s).These devices and their peripherals are remotely attackable.
- Any USB device connected to a hardware asset that has an IP address. These devices are a vector to spread malware among devices.

This definition is used by FISMA and is documented on page 23 of the annual FISMA reporting instructions.

Thus, not every "device" in a property inventory is included in the Hardware Asset Management definition of devices. For example, a monitor (not addressable, thus not included) can be attacked only through an addressable computer. For other examples, see the FISMA reporting instructions.

If you find other kinds of devices that you believe should be included, please let us know so we can consider those issues.

8. QUESTION: WHEN IS A DEVICE CONSIDERED AUTHORIZED?

Answer: A device is considered authorized when it has met authorization criteria and gained approval to be connected to your network. In most agencies, new systems must go through a certification and authorization process before being authorized to connect.

Links to Related Resources
NIST Guidance:
• NIST 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems

9. QUESTION: WHAT IS THE HARDWARE ASSET MANAGEMENT DESIRED STATE?

Answer: The Hardware Asset Management desired state is a list of the hardware assets (devices) you expect to find on the network.

The list of desired state hardware assets should
- *be created through a repeatable process*
- *include only authorized devices*
- *assign each authorized device for technical management of settings, software, patching, etc.*

Because it is important to find unauthorized devices quickly, the list of authorized devices should be stored in a data format that is easy to compare to actual inventory via automation, so unauthorized devices can be easily identified. Manual comparison is too slow and expensive in comparison to the pace of cyber attacks.

A network sensor tool like a scanner or passive listener cannot identify authorized or managed devices unless each device has an encrypted and signed certificate. Because this strategy is not generally available in the short term, the desired state inventory is usually created using an inventory database of some type.

10. QUESTION: WHAT DATA SHOULD BE RECORDED IN THE HARDWARE ASSET MANAGEMENT DESIRED STATE INVENTORY?

Answer: The minimal Hardware Asset Management data recorded for desired state devices should include the following:

Data Item	Justification
Expected CPE (vendor, product, version, release level) or equivalent	• For reporting device types • For supply chain management • To know what CVEs may apply to these devices
Person or organization who is responsible for managing the hardware asset (note: such assignments should ensure that the designee is not assigned too many assets to effectively manage them)	• To know who should fix specific risk conditions • To assess the responsible individuals' risk management performance
Data necessary to link desired state inventory to actual state inventory	• To be able to identify unauthorized and unmanaged devices
Data necessary to physically locate hardware assets	• So managers can find the device to fix it • To identify mobile devices so that extra controls can be assigned
The period of time the asset is authorized	• To allow previously authorized devices to remain in the inventory, while knowing they are no longer authorized
Expected status of the device (active, inactive, stolen, missing, transferred, etc.)	• To know which authorized devices are not likely to be found in actual inventory
Data necessary to physically identify the asset (such as property number or serial number)	• To be able to validate that the remotely found device is actually this device, and not an imposter

This minimal list of data items is a starting point. There are many operational and security concerns for which more data may be required.

Links to Related Resources
NIST Guidance:
• NIST Interagency Report 7693 - Specification for Asset Identification 1.1

11. QUESTION: HOW CAN AN ORGANIZATION DETERMINE ITS DESIRED STATE?

Answer: See the solutions below.

Background: Because so few networks are centrally managed, the idea of having hardware inventory data can seem infeasible. In some environments where staff move around considerably (e.g., emergency management programs, troop deployments) and take equipment with them, inventory can be especially hard to manage. For many agencies with legacy networks without a prior Hardware Asset Management program, getting a large number of legacy devices into a desired state inventory and assigned is daunting. These are all legitimate concerns, but there are solutions.

Solutions:

1) Approval of inventory can be de-centralized. For example, if a person is authorized to install new equipment, they should have the authority to add it to authorized inventory (or for separation of duties, as appropriate, a second person could add it to inventory for them).

Hardware Asset Management does not require centralized control of desired state inventory. Centralized control of desired state inventory is infeasible in most large organizations.

2) Legacy equipment can be identified to be put into authorized inventory by using data from the actual state inventory. A manual process is normally needed to collect data about the device for the desired state inventory.

3) Legacy equipment can often be assigned for management, at least initially, based on one of the following criteria:

- An IP range to be managed by a certain group
- An LDAP structure like an Active Directory "organizational unit" used to assign privileges needed to administer the device
- Where the device is physically located
- What switch or router connects the device to the network
- Data on some devices may be in property and procurement management systems (but rarely helps define who manages the device)

4) After legacy equipment is initially assigned for management, managers can be asked to verify the assignment or help identify the correct manager if the assignment is incorrect. Experience has shown that applying this heuristic process to assignments can make great improvements in accuracy: initial assignments that are only 70% correct can be improved through 98% correct in a few months of careful effort.

12. QUESTION: HOW SHOULD/COULD AN ORGANIZATION ASSIGN MANAGERS FOR HARDWARE ASSET MANAGEMENT ASSETS?

Answer: Organizations should assign managers to meet the definitions described below. These assignments should be recorded in the desired state inventory.

Definitions:

The manager of the IT asset is the group of persons who have authority and responsibility to manage the device.

Managing the device means, at a minimum:

- Connecting the device to the network
- Configuring its operating system

Managing the device typically also includes the following, but these responsibilities may be matrixed. Risk transfers can be used to deal with such exceptions.

- Making adjustments to the operating system settings and/or patching to support a specific application(s)
- Controlling other software installation on the device
- Keeping patching up to date
- Managing settings of the other software

Authority and responsibility means, at a minimum, having the right administrator privileges on the device to manage a device. (For automated functions, those who manage the tools that automate the process are the managers for the items automated.)

While the assignment process is normally manual, there is some potential to automate it. For example, where LDAP data defines groups of devices and who manages them, the LDAP data can be read so that when new devices are added to a device group, the device can automatically be assigned to the administrator group that manages that device group. Likewise, when a person is removed from the administrator group, he/she is no longer responsible for managing the devices in the covered device groups.

The following are NOT the actual managers of a device (unless they also meet the criteria above, which might happen in a micro-agency):

- People who supervise the group of individuals who have authority and responsibility to manage the device

- The CISO and/or CIO who covers the device

- Other managers who are not actually device or software administrators

- The user of the device

- The business owner of the device or the applications on it

Manager identification must be used to know which individual(s) is/are responsible for specific risks and can be expected to fix risk conditions.

Once CDM is in place, devices without an assigned manager (individual or group) will be scored as a risk because they are not managed. One way to "game the system" is to assign all devices to one person, whether or not that person actually manages the devices. This does not reduce the risk and will be identified in the dashboard reports. (The dashboard produces reports on the number of devices covered by each manager to help the organization balance workload.)

13. QUESTION: CAN I SIMPLY USE MY PROPERTY MANAGEMENT SYSTEM AS DESIRED STATE?

Answer: In theory, your property management system should be able to tell you the devices owned by the organization. It is especially helpful if your property management system can tell you the expected configuration of the hardware. In practice, there are typically many limits to using property system data. The property system may not be able to answer the following questions:

- Which network is the device connected to, if any?
- Who manages the device? (A property management system is more likely to identify the purchaser, who might be the business owner or the CIO.)
- Has the device has been retired, lost, or stolen?
- Where is the device physically located?

The property system will also include "devices" like monitors and keyboards that are not included in the CDM actual state inventory. In many agencies, where procurement and property management are distributed, there may be no central repository of property data, or the central

repository may be incomplete. Collecting data from distributed property systems with differing data quality and format may be difficult and misleading.

Recommendation: Each agency should carefully consider the advantages and disadvantages of using property data to help populate its desired state inventory. Such data should be used only where practical.

*An organization's property management system tracks hardware asset **ownership**, which is different from Hardware Asset Management, which tracks **management** of hardware assets.*

14. QUESTION: IS NETWORK ACCESS CONTROL (NAC) A GOOD SOLUTION FOR ACHIEVING HARDWARE ASSET MANAGEMENT?

Answer: Normal implementations of NAC are not a complete solution for achieving Hardware Asset Management for two reasons. First, NAC tends to ignore whether the device is officially authorized or assigned a manager before allowing it to connect to the network. Second, once a device is deemed by NAC to be in compliance, it is usually not rechecked to ensure it remains in compliance. CDM requires that hardware assets are on the network only for the time that they are authorized according to an organization's management process.

NAC solutions are a way to force assets to "comply to connect" to the network. Hardware Asset Management is about ensuring appropriate management of a hardware device, not compliance and meeting minimum network standards.

5 ACTUAL STATE

15. QUESTION: WHAT IS THE HARDWARE ASSET MANAGEMENT "ACTUAL STATE"?

Definition: The actual state is the set of all devices actually on the network at any moment. The actual state includes all authorized, unauthorized, managed, and unmanaged devices on the network.

Definition: The actual state inventory is the best available list of the current actual state devices.

The primary purpose of the actual state inventory is to quickly identify all devices on the network to ensure that they are authorized and/or managed. Unauthorized and unmanaged devices must be either removed or authorized and managed.

A secondary purpose is to identify missing devices that may have been lost or stolen (i.e., devices in the desired state inventory, but not actually on the network).

The actual state inventory process must be fast enough to find and address unauthorized, unmanaged, and/or missing devices before attackers can find and exploit them. Because attackers are constantly searching for these devices via automated means, manual methods are not fast enough to reduce likelihood and impact of system compromise.

16. QUESTION: HOW DOES AN ORGANIZATION DETERMINE ITS HARDWARE ASSET MANAGEMENT ACTUAL STATE?

Answer: The CDM program has established a strategically-sourced procurement to provide sensors to collect data about devices actually on the network (and to provide operation of the sensors). These sensors perform periodic device discovery through listening, scanning, device self-reporting, and other means.

As of 2013, most agencies have some tools to help identify the devices actually on their networks. Many more lack a way to know the desired state and compare it to this actual state. Without both inventories, it is not feasible to identify missing, unauthorized, or unmanaged devices.

*In the future, **scanning will become a less viable way** to execute Hardware Asset Management. This is because the IPv6 Address space is so large that scanners will not be able to find devices quickly enough. In addition, scanning tends to miss devices in unexpected IP ranges.*

The list of actual state devices should be stored in a data format that is easy to compare to desired inventory, so unauthorized devices can be easily found.

17. QUESTION: WHAT DATA SHOULD BE RECORDED IN THE HARDWARE ASSET MANAGEMENT ACTUAL STATE INVENTORY?

Answer: The minimal Hardware Asset Management data recorded for actual state devices should include:

Data Item	Justification
Expected CPE (vendor, product, version, release level) or equivalent	• For reporting device types • For supply chain management • To know what CVEs may apply to these devices
Data necessary to link desired state inventory to actual inventory - Serial number - Model number - Static Internet protocol (IP) address (for network-accessible assets) - Media access control (MAC) address (for network-accessible assets)	• To be able to identify unauthorized and unmanaged devices or to find missing or lost devices
Data necessary to locate the actual hardware asset	• So managers can find the device to fix it

This minimal list of data items is a starting point. There are many operational and security concerns for which more data may be required.

Links to Related Resources
DHS/FNR Guidance:
• HWAM Foundational Survey, questions 16-18 [Link]
NIST Guidance:
• NIST Interagency Report 7693 - Specification for Asset Identification 1.1 http://csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf

If you collect other data you think is essential and/or useful, please document it and let us know so we can report your ideas here for other organizations to consider.

6 FINDING RISK CONDITIONS AND DEFECTS

18. QUESTION: HOW DOES AN ORGANIZATION FIND THE DIFFERENCE BETWEEN DESIRED STATE AND ACTUAL STATE IN HARDWARE ASSET MANAGEMENT?

Answer: If the desired state inventory and actual state inventory are set up correctly, all the data necessary to detect these potential risk conditions is available, and detection can be done with a simple database query. Findings can then be reported to a dashboard, which can record when the risk condition was found and how long it existed. **Under CDM, this process is automated and handled by the CDM dashboard once data is received from the desired state inventory and the actual state sensors.**

Definition: A difference between the desired state and the actual state is considered a risk condition. Primary examples are listed in the table below:

Difference detected between desired and actual state	Why is this considered a risk condition?	What is the likely risk?
A device is actually on the network, but NOT in desired state inventory.	We can't know who is managing the device or whether the device is authorized.	It is highly probable that the device is highly vulnerable and can be easily compromised if detected by an attacker.
A device is in desired and actual state inventory, but no one is assigned to manage the device.	We can't know who is managing the device.	It is highly probable that the device is highly vulnerable and can be easily compromised if detected by an attacker.
A device is in desired state inventory, but not in actual inventory.	There are two possibilities: • The device may not be reporting, which would reduce our account for it in other areas. • The device may have been lost or stolen, along with the data on the device.	There are two possibilities: • The device needs to be back in reporting status. • The device needs to be found to protect the data on the device. If either is the case, the device could be easily compromised if detected by an attacker.

To find the differences between desired and actual state inventory, you must have a consistent way to identify devices in both inventories. Actual state detectors usually have the easiest time identifying IP address, but if the IP address of a specific device changes frequently, this may not be the best identifier. Other alternatives are machine name and MAC address.

19. QUESTION: WHY IS THE GAP BETWEEN DESIRED STATE AND ACTUAL STATE IMPORTANT?

Answer: This is largely answered in Question 18. Gaps between desired and actual state are important because they indicate the presence of unmanaged hardware assets that can be vulnerable to attack.

Knowing who manages each device is crucial to effective endpoint security. This applies not only to HWAM, but also to SWAM, CSM, and VUL. If we don't know who is responsible, the dashboard cannot be configured to send messages about risk conditions to the right people to fix the problem.

7 FIXING DEFECTS

20. QUESTION: HOW CAN AN ORGANIZATION ADDRESS THE DIFFERENCE BETWEEN ACTUAL AND DESIRED STATE?

Answer: Once the CDM dashboard has identified the differences between actual and desired state inventories, it will mark difference as risk conditions (defects). Scoring algorithms will be applied to estimate the risk posed by this defect. The risk score may be higher if the risk condition is older (as the probability of compromise increases) or if the risk condition is associated with active or high-impact attacks. Certain kinds of devices may also get a higher score.
For example,

- A "rogue" device with a link to the Internet would present a higher risk than one without such a link.
- A missing or "rogue" device known to hold sensitive data would present a higher risk than most devices.

Actual removal of the risk requires the following actions:

Risk Condition	Typical Mitigation (though acceptance of risk is an option)
Device is unauthorized (not in desired state inventory) and therefore unmanaged.	Option 1: If the device should be on the network, authorize it, add it to desired state inventory, and assign it for management. Option 2: Remove the device from the network.
Device is authorized (in desired state inventory), but no manager is assigned.	Option 1: If management has already been assigned, identify the manager and record the result in desired state inventory. Option 2: Assign the device to an appropriate manager and record this in desired state inventory. (This manager will be informed of other risk conditions on the device so they can be addressed.)
The device is in desired state inventory but doesn't appear in actual state inventory.	Option 1: If the device is actually on the network but not reporting (being detected), this is a sensor problem. Work with the sensor managers to fix whatever is blocking detection. Option 2: The device may be lost or stolen. Investigate the cause. If already lost or stolen, record this as an incident, and update the device status in the desired state inventory.

Tracking Actions: After these mitigation actions are taken, the changes to the desired and actual state inventory will cause the risk condition to disappear when the next round of sensor data is collected and sent to the dashboard. As a result, there is no need to track this work as a task (or to record when completed) in a ticketing system because CDM will track it until completed.

Cognizant Manager(s): Because most of the risk conditions addressed in HWAM involve unmanaged devices, the risk score cannot be sent to the device manager. This means that the organization needs a separate team to address unassigned devices. The dashboard will then send this kind of risk condition to this team until the device is assigned for management. In some organizations, these assignments might be by divided by domain or some other network topology feature to allow distribution of this work across the larger enterprise.

Prioritization: These same risk managers need to be able to see other risk conditions on these devices (typically, software, patching/vulnerabilities, and settings) in order to prioritize Hardware Asset Management risk conditions. If data is available on the impact of compromises of data on each machine, the lost device issues can also be prioritized.

21. QUESTION: HOW CAN WE PREVENT UNAUTHORIZED DEVICES FROM GETTING ON THE NETWORK IN THE FIRST PLACE?

Background: Removing/assigning unauthorized devices should theoretically not be necessary. But in real operational networks, it often seems inevitable. Organizations can take particular steps to reduce the work required to find out who is responsible for these devices and to record this data.

Answer: The following kinds of actions can be taken to reduce the number of unauthorized and unmanaged devices that appear on the network:

1) **Policy can require administrators to put new devices into desired state inventory before adding them.** Often system administrators connect new devices, then patch and configure them on the production network. This provides a window for the devices to be compromised. In addition, the devices are often added to the network before being recorded in active directory (or whatever other source of data for desired state is in use). Getting administrators to keep the desired state up-to-date (edited before the machine appears) will reduce the number of Hardware Asset Management risk conditions.

2) **Logging can track when unauthorized and unmanaged devices are connected to the network, what they are connected to, and who has logged onto them.** All of this data can help investigate who connected the devices. Once the person is found, letting them know what is expected can prevent creation of these risk conditions.

3) **A few people may need to be sanctioned.** Sanction individuals who frequently connect unauthorized devices, and who do so after due warning.

While such actions won't eliminate all unauthorized and unmanaged devices, these actions can lower their incidence rates, which it a positive step.