Home Office Network Asset Inventory

Introduction

In a small home office, multiple devices are connected to a network. Each device represents a potential entry point for security threats, and many store sensitive information that could impact the business if compromised. Maintaining a **network asset inventory** helps identify which devices require extra protection.

This document provides a **detailed inventory of network devices**, their characteristics, notes on network access, and classification of sensitivity levels.

Step 1: Identify Assets

I identified **three additional devices** on the home network that are not already listed in the template. The chosen devices are:

1. **External Hard Drive**
2. **Smart Webcam**
3. **Smartphone**

Step 2: Device Characteristics

For each device, the following characteristics were recorded:

Asset	Network Access	Owner	Location
External Hard Drive	Occasionally connected via USB, sometimes accessed via network for backups	Abdullah	Next to desktop on office desk

Smart Webcam	Always connected to network for monitoring	Abdullah	Living room, facing entrance
Smartphone	Always connected via Wi-Fi, syncs with cloud	Abdullah	Pocket, desk, or carried around

Explanation of characteristics:

- **Network Access:** Describes how often and in what way the device connects to the network. This helps evaluate potential exposure to security risks.
- **Owner:** Identifies the person responsible for maintaining the device and securing the data.
- **Location:** Physical proximity to the router affects connectivity and possible interference; also determines physical security risk.

Step 3: Evaluate Network Access & Notes

Here are detailed notes for each device regarding their network access and potential risks:

Asset	Notes
External Hard Drive	Contains sensitive business documents and backups. Connected occasionally via USB, sometimes shared over local network. Needs protection from unauthorized access.
Smart Webcam	Continuously streams video to cloud. Can be accessed remotely. If compromised, could reveal physical office setup or personal activities.
Smartphone	Synchronizes emails, business apps, and cloud storage. Frequently used outside home, increasing risk of exposure to public networks or phishing attacks.

Notes Explanation:

- Each note highlights **confidentiality, integrity, and availability (CIA)** concerns:
  - **External Hard Drive:** Confidentiality is critical; integrity if files are modified.
  - **Smart Webcam:** Confidentiality risk if video is leaked; availability important for continuous monitoring.
  - **Smartphone:** Confidentiality and integrity critical due to emails and cloud sync; availability is important for business communications.

Step 4: Sensitivity Classification

Based on the potential impact on the business if a device is compromised, the devices are classified as follows:

Asset	Sensitivity Level
External Hard Drive	Highly Confidential
Smart Webcam	Confidential
Smartphone	Highly Confidential

Classification Rationale:

1. **External Hard Drive:**
   - Contains business documents, client information, and backups.
   - If stolen or modified, could severely impact business operations.
   - **Level:** Highly Confidential.
2. **Smart Webcam:**
   - Streams video to the cloud; mainly monitors office.

    - Compromise would lead to potential privacy breaches but limited direct business data loss.
    - **Level:** Confidential.

3. **Smartphone:**
    - Accesses emails, apps, cloud storage.
    - Losing control or data breach could expose sensitive information and disrupt communications.
    - **Level:** Highly Confidential.

Step 5: Summary & Recommendations

Summary

This inventory identifies **three devices** on the home office network, evaluates their **network access, ownership, and physical location**, and assigns **sensitivity levels** based on their potential impact if compromised.

Asset	Network Access	Owner	Location	Notes	Sensitivity Level
External Hard Drive	Occasionally connected via USB, sometimes accessed via network for backups	Abdullah	Next to desktop on office desk	Contains sensitive business documents and backups. Needs protection from unauthorized access.	Highly Confidential

Smart Webcam	Always connected to network for monitoring	Abdullah	Living room, facing entrance	Continuously streams video to cloud. If compromised, could reveal office setup.	Confidential
Smartphone	Always connected via Wi-Fi, syncs with cloud	Abdullah	Pocket, desk, or carried around	Synchronizes emails, business apps, and cloud storage. Risk if lost or exposed to public networks.	Highly Confidential

Recommendations

1. **External Hard Drive:**
    - Encrypt files and enable password protection.
    - Limit network sharing.
2. **Smart Webcam:**
    - Use strong, unique passwords and two-factor authentication (2FA) for cloud access.
    - Keep firmware updated.
3. **Smartphone:**
    - Enable device encryption and 2FA for all business apps.
    - Install mobile security software and avoid connecting to public Wi-Fi without VPN.

Step 6: Save & Maintain Inventory

- Save a copy of this inventory in a secure location (cloud + local backup).
- Update inventory whenever new devices are added or removed from the network.
- Review sensitivity classifications periodically to reflect changes in device usage or business requirements.

Conclusion

Creating a **network device inventory** helps a small business identify sensitive assets, understand potential risks, and implement appropriate protections. By classifying devices by **sensitivity**, owners can prioritize security measures to reduce the likelihood of data breaches and operational disruptions.