Personal Asset Inventory Assignment

Jim Kinter

CIDM6341

1. What did you do?

I conducted a comprehensive asset inventory using a methodical, data-centric approach aligned with NIST Cybersecurity Framework (CSF) principles, particularly under the "Identify" function for asset management. I defined key asset categories: people, hardware, networking devices, software, data, procedures/routines, systems, transportation, and equipment.

For people, I reviewed my phone's contact list, which contains 5320 professional contacts, but focused on personal and familial relationships comprising 12 people: my father Bill and his wife Claudia (not my mother), two living cousins Paula and Joe, four children (Josh age 21 not at home, Ben age 20 at home/college, Sarah age 17 at home, Sam age 13 at home), a spouse Kristie age 51, two in-laws (Gerald age 82 and Kathy age 68 living with us), a brother-in-law Gerald Wayne, and a nephew Ethan. I also quantified social media networks: LinkedIn (3777 contacts), Facebook (661 contacts), and X (397 followers), treating these as extensions of people-related assets for potential risk assessment.

For hardware and networking devices, including IoT devices and cameras, I utilized Advanced IP Scanner, a free, simple, and Windows-compatible tool, to interrogate my home network. I installed Advanced IP Scanner on my Windows laptop, scanned the local network, and reviewed the output (provided as NetworkScan.html) to generate a detailed list of all connected devices, including their IP addresses, manufacturers, MAC addresses, and services (e.g., HTTP, Radmin). This allowed me to identify specific assets like the NETGEAR Orbi router, Ring devices, HP printer, Amazon Echo devices, Whisker Labs Ting sensors, and others, mapping them to categories. For devices not appearing in the scan or not individually detected (e.g., Calix modem, Ubiquiti radios, third Ting, second Samsung TV, XBox One, multiple Ring cameras, additional Amazon Echos, Chamberlain smart Garage Door Opener), I included them based on manual verification and knowledge of the setup, such as counting and locating the six Ring cameras (Front Doorbell, East Steps, West Well, Back Door, Pool, Back Steps) and seven Amazon Echo devices (Family Room, Kitchen, Master Bedroom, Office, Sam's Room, Sarah's Room, Back Porch). Vendors for unidentified MACs were cross-referenced with online MAC lookup resources to assign likely types (e.g., Espressif for IoT).

For software, I systematically inventoried applications on my laptop (total 60 apps) by exporting the installed programs list via the operating system's control panel and categorizing them into 28 frequently used (e.g., browsers, office suites) and 32 infrequently used (including TurboTax). Similarly, for my iPhone 15 Pro Max, I reviewed the app library and settings to count 187 apps, grouping them into 14 frequently used (e.g., messaging, email, including DayOne app used for over 5 years for daily diary) and 173 infrequently used.

For data and physical records, I conducted a room-by-room inspection of my house, systematically going through every drawer, box, file cabinet, folder, and (most importantly) my safe in order to catalog items such as birth certificates, vaccination records, insurance statements, mortgage statements, equipment warranties (washer, dryer, refrigerator, air conditioner), bank statements, investment account statements, maintenance contracts, loan documents, and current and prior year’s tax returns (both physical and digital). Digital data was cross-referenced with repositories like cloud storage, email archives, password managers, and DayOne diary entries for routine verification. Equipment and assets in the pool house that belong to my in-laws (washer/dryer, TV, applicances) were intentionally excluded from the inventory.

For procedures, I documented routines based on logs, habits, and over 5 years of entries in the DayOne app on my iPhone, which provided detailed insights into recurring activities like backups, password changes, software updates, family communication protocols, physical security routines, online shopping procedures, social media highlights, and vehicle maintenance logging.

For transportation and equipment, I manually listed vehicles (cars, trucks, motorcycles, trailers) and non-transportation items (Kubota Ranger, Simplicity Broadmoor lawnmower, Echo Weedeater, Echo Chainsaw, Craftsman Chainsaw, Black & Decker Weedeater, Black & Decker Electric Mower, Toro Push Mower, Ryobi Weedeater, Generic Rototiller, Bilt Hard Log Splitter, Makita Drill, Craftsman Drill, Ryobi Power Washer, Ryobi corded circular saw, Ryobi cordless blower, Ryobi Cordless Sawzall, Ryobi Cordless Jigsaw, generic air compressor, Motobecane Turino XL Road Bicycle (Black), Motobecane Mountain Bicycle (Black), Motobecane Mountain Bicycle (Blue), Specialized Mountain Bicycle (White)) by conducting a physical inventory, inspecting garages, sheds, and storage areas to catalog each item.

To group assets, I used a hierarchical method: prefix-based categorization (P for people, H for hardware, T for transportation, E for equipment, etc.) for unique IDs, then assigned System IDs based on functional interrelations per NIST CSF functions. Assets fitting multiple groups (e.g., a smartphone as hardware with software and data, including DayOne diary data) were assigned a primary category by core function (hardware) and linked to the dominant system (SYS3 for mobile), with overlaps noted in descriptions and system definitions to maintain relational integrity without duplication. I iterated the process, cross-verifying categories for completeness, and incorporated specifics from the network scan and manual additions to refine device identifications.

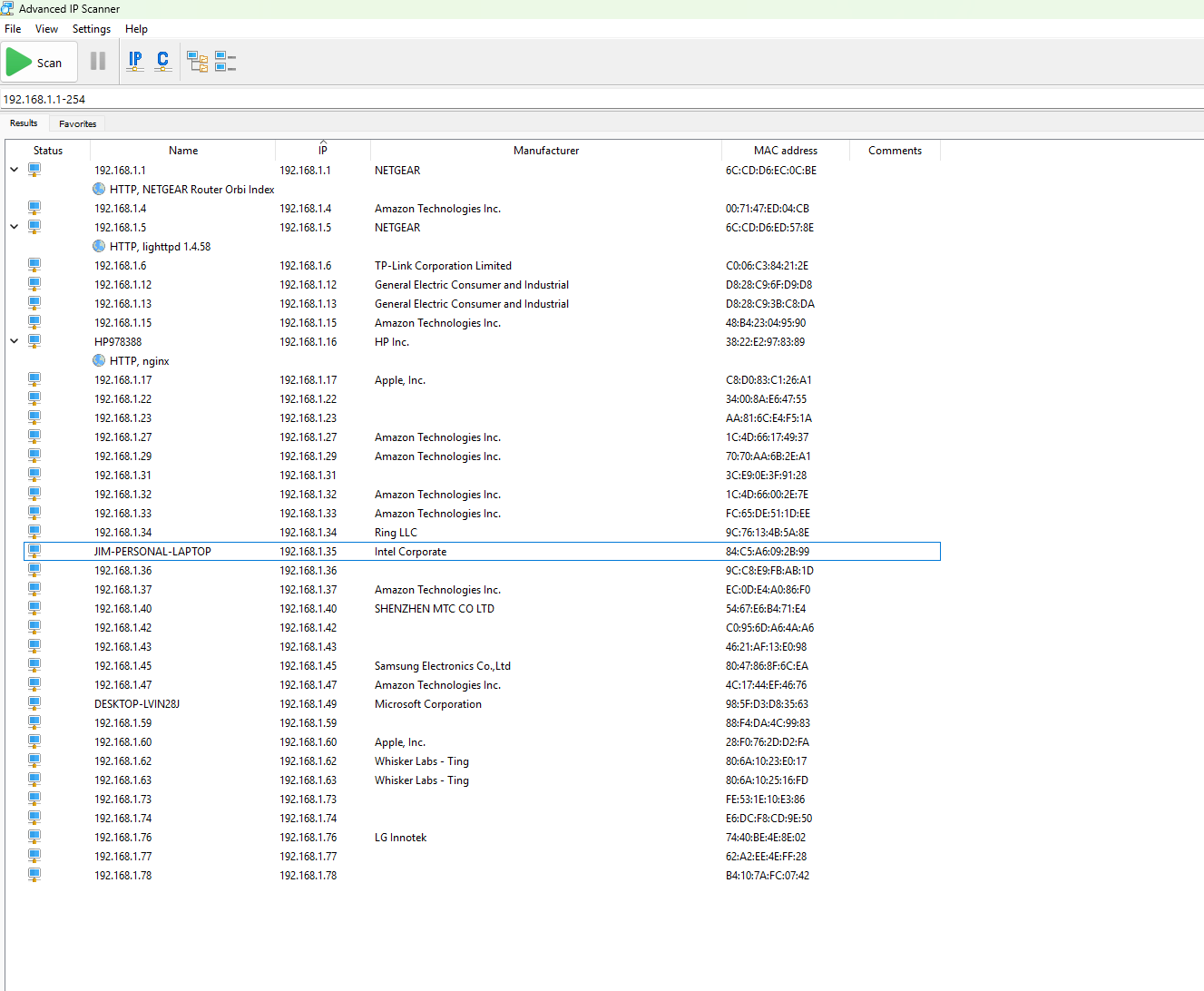


Figure Network Scan

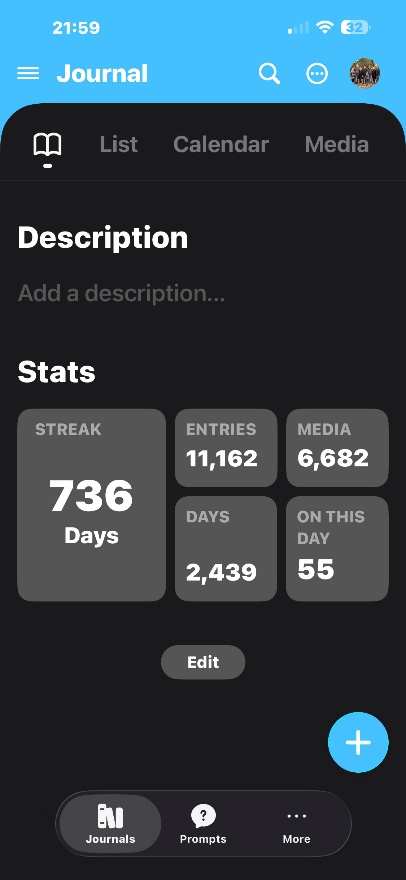


Figure DayOne Statistics



Figure My personal fire safe

1. What Are the Results?

The inventory produced a catalog of assets across categories, grouped into 13 systems. This reveals an extensive attack surface: people (14 entries, plus social media metrics) highlight social engineering risks, especially with multi-generational household including elderly in-laws; hardware (9, including trackers and non-network devices) and networking/IoT (34, refined from scan like Ting sensors, GE appliances, Samsung TVs, XBox One, multiple Ring cameras, seven Amazon Echos, Chamberlain opener, and added Ubiquiti radios/Calix modem) indicate network vulnerabilities from numerous interconnected devices (e.g., 30+ from scan plus additions); transportation (8 vehicles, including trailer) and equipment (23 items, expanded with tools and bicycles) add physical risks; software (7 grouped entries, totaling 247 apps, including DayOne) exposes risks from infrequently used items; data (16, including 7 years of tax returns and DayOne diary data) underscores sensitive information exposure; procedures (8, informed by DayOne entries) identify behavioral gaps. Systems like SYS5 (Network) and SYS8 (Social Media) expand the surface through connectivity—a breached Orbi router could compromise all scanned devices including multiple cameras and Echos, while large social networks (e.g., 3777 LinkedIn contacts) increase phishing vectors. Physical records, vehicles, and equipment add offline risks, like theft of hard copies, vehicle-related documents, or tools.

1. What Did You Learn?

My attack surface is significantly larger than I expected. This is driven by extensive social media connections, numerous infrequently used apps (205 across devices), interconnected IoT/network devices identified (e.g., multiple Amazon and unidentified devices now vendor-mapped like Espressif IoT), a multi-vehicle, multi-tracker setup with AirTags, multiple Ring cameras, seven Amazon Echo devices, and additions like Ubiquiti radios, multiple Ting devices, an XBox One, Chamberlain smart Garage Door Opener, non-transportation equipment including tools and bicycles, and sensitive data in DayOne diary entries. I have more risk than anticipated, particularly from physical records scattered across the house, dormant software that could harbor vulnerabilities, diary data containing routine details, and household devices/equipment accessible to family members of varying ages and tech-savviness. This underscores the value of regular audits, app pruning, network segmentation, centralized physical storage, securing diary data, and family education on security to mitigate risks. It’s time to revisit my personal security and pare this footprint back again.