VITAL CYBER
Provided by MCNC

Episode 2: Enterprise Asset Management

Question about a term?
Visit our Glossary

Welcome to episode two of our blog series, "Cybersecurity 101: Securing Your Digital Environment." In this episode, we're diving into a topic that doesn't always get the spotlight—Enterprise Asset Management (EAM). Sure, it may not get the same recognition as the latest threat detection tools or firewalls, but EAM is one of the three foundational topics of your cybersecurity program. The other two? Software Asset Management (SAM) and Data Management (DM), but we'll discuss those later. Without EAM, your organization could be open to risks like data breaches and compliance failures. Mastering EAM is essential to securing your environment.

What's Enterprise Asset Management?

You might be wondering, **What exactly counts as an 'enterprise asset'?** Think of an asset as anything useful or valuable to your organization. In the context of EAM, we're talking about any enterprise-owned or otherwise authorized device—whether it's physical, virtual, cloud-based, local, or remote—that has the potential to create, store, or transmit data. This includes everything from desktops and laptops to servers, tablets, printers, network and IoT devices. Enterprise Asset Management (EAM) is the procurement, identification, tracking, maintenance, and eventual disposal of these devices. But don't mistake EAM for just keeping a list of your equipment; it's a comprehensive, ongoing process that follows each asset throughout its entire lifecycle.

Sounds good, but why is EAM important? Without a strong EAM process, organizations may have blind spots within their environment, making them more vulnerable to events that could lead to an incident. For example, an organization without an EAM process could have unaccounted-for devices in their environment, some of which could contain sensitive data. If one of these devices were lost or stolen, it could lead to a data breach. Who was responsible for the device? What data was stored on the device? Was it encrypted? If so, is it documented? In a suspected data breach situation, providing these answers is critical in determining the next steps and, ultimately, the event's impact. That's one of the reasons why it is essential to have a solid EAM process that tracks and updates your enterprise assets' status throughout their life.

The Framework

Before you begin building out the EAM process, let's review what CIS version 8.1 safeguards in the framework should be addressed.

- **Basic Cyber Hygiene (IG1).** The road to basic cyber hygiene starts with an EAM process that includes:
  - (CIS 1.1) Establishing and maintaining a detailed enterprise asset inventory
  - (CIS 1.2) Identifying and addressing unauthorized assets
  - (CIS 3.5) Ensuring appropriate asset disposal based on data sensitivity.
- **Additional Safeguards (IG2).** To further improve the EAM process, you can implement safeguards that use:
  - (CIS 1.3) An active discovery tool to identify assets connected to the enterprise network
  - (CIS 1.4) DHCP logging to update your organization's enterprise asset inventory more efficiently.

Where To Start?

Alright, we now know what the EAM process needs to achieve, but where do we start? First, to get the EAM process off the ground, we suggest formally establishing in your organization the basic cyber hygiene safeguards we've mentioned, plus any others that make sense. The best way to do this is to develop solid policies, standards, and procedures around these topics.

- **Policy.** The first step in setting up your EAM process is to lay down a clear policy, approved by senior leadership, that serves as the backbone for everything that follows. This policy should define who's in charge of the EAM process, who's handling the day-to-day management of assets, and what is expected at each stage of an asset's life cycle. By answering these questions upfront, you ensure that everyone's on the same page and that your approach to asset management is consistent across the board. Need help getting started? Here's a template we've created with the essentials to get you started.
- **Standards and Procedures.** Standards and procedures take your policy from paper to practice, giving you a clear roadmap for daily operations. Need a kickstart? Here are our templates for standards and procedures to point you in the right direction.

Where Do We Go From Here?

Now that we have our administrative controls, it's time to put them into practice. Start by inventorying your enterprise assets. Once that's done, manage your assets throughout their lifespan and update the inventory as needed.

- **Create an Up-To-Date Inventory.** As you likely already have dozens of enterprise assets in your environment, and it's hard to protect assets you do not know about, we recommend performing everyone's favorite activity, inventory. Although hated by many, starting with an accurate account of all enterprise assets is fundamental to establishing an effective EAM process. To perform this task, you can use automation with specialized software or the manual spreadsheet method. If the latter suits you, here is our template with the essential asset categories to get you started.
- **Managing Your Assets.** Staff should follow defined policies, standards, and procedures to manage assets through their lifecycle, including:
    - **Acquisition.** Vet potential vendors and inventory new asset acquisitions.
    - **Discovery.** Identify unknown devices found in the organization's environment. Add authorized assets to the inventory and address any unauthorized assets. Discovery tools such as NMAP or Zenmap are open-source resources you can leverage for this task.
    - **Usage.** Establish an Acceptable Use Policy (AUP) to outline rules and responsibilities for employees and authorized users. Make sure users are aware of and affirm that they understand their responsibilities. Here's our template to get started if you need one.
    - **Disposal.** Properly retire assets to ensure secure data disposal.

Where We're At!

Building upon the Cybersecurity Framework we provided in episode one, here is a visualization of the progress made in episode one and two.

Take the Next Step in Strengthening Your Cybersecurity

Is your organization ready to enhance its cybersecurity posture? Our team of experts at MCNC is here to help. Whether you need a comprehensive risk assessment, policy analysis, or guidance on implementing best practices, we're ready to partner with you to safeguard your digital assets.

Don't wait until it's too late. Contact us today to schedule a consultation and discover how MCNC's Vital Cyber solutions can protect your institution. Fill out our Contact Us form and let's start building a stronger defense together.