Asset Management: A Cornerstone of Cybersecurity

What our suppliers need to know

Asset management is a critical discipline for any organisation seeking to establish and maintain a robust cybersecurity posture. It provides the foundational visibility and control necessary to effectively manage risks, protects resources and sensitive data, and supports operational resilience.

What Are Assets?

An “asset” is something that produces value for your organisation, such as intellectual property or customer data, technology and your people, and their knowledge and skills. Information Technology (IT) and Operational Technology (OT) assets include:

- **Hardware:** Servers, workstations, laptops, mobile devices, network equipment (routers, switches, firewalls), printers, peripherals, Internet of Things (IoT) devices, Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), etc.
- **Software:** Operating systems, commercial and open-source software, databases, middleware, firmware, and related license information.
- **Cloud resources:** Virtual machines, cloud instances, containers, storage, and software-defined networking, and software application components.

Data, information, and knowledge are also critical assets for your organisation. You should know your data’s location and classification, and who has access. Data governance is closely related to asset management.

What Is Asset Management?

“Asset management” is the process of tracking and managing IT, OT, and data assets throughout their lifecycle, from procurement to disposal. It involves establishing policies, procedures, and tools to effectively acquire, deploy, maintain, upgrade, and dispose of assets.

Why Is Asset Management Important?

From a business perspective, asset management optimises resource allocation, reduces unnecessary spending, and improves operational efficiency by providing a clear understanding of an asset’s lifecycle and utilisation. From a cybersecurity perspective, it is fundamental for vulnerability management, incident response, and compliance, improving visibility and control to secure and protect critical systems and data.

Done well, it results in:

- **Reduced Security Risks:** Knowing what assets you own, where they are, and their security status is essential to identifying and mitigating vulnerabilities. Unmanaged or unknown assets (e.g. “shadow IT”) are prime targets for attackers.
- **Improved Compliance:** Asset management is a key component of compliance to regulations, standards, and customer requirements (e.g., NIST 800-171, DefStan 05-138, ISO 27001, etc.). It requires you to demonstrate responsibility for your assets and provide the necessary documentation and evidence of the audit processes.
- **Optimised Resource Allocation:** Asset management helps your organisation avoid unnecessary purchases, optimise software licensing, and ensure that your resources are allocated efficiently. This frees up your budget for other investments.
- **Improved Incident Response:** During a security incident, having an accurate inventory of assets enables faster containment and recovery. Knowing which systems are affected and their dependencies helps you to prioritise your response efforts.
- **Better Vulnerability Management:** Asset management is essential for effective vulnerability management. Knowing your software and operating systems and their patch levels can help you prioritise patching and remediation efforts.
- **Improved Software License Management:** Effective asset management helps you avoid software license violations, which can result in legal and financial penalties.

Additionally, asset management supports configuration management: Your configuration management database (CMDB) should record information about your hardware, software, and virtual assets. This is essential for maintaining consistent and secure system configurations.

Good asset management means creating, establishing, and maintaining accurate information that supports day-to-day operations and efficient decision making.

How to Perform Asset Management

Initiating and operating an effective asset management program is not difficult, but it does require diligence and attention to detail at the executive, managerial, and production line levels. Here are key steps:

1. **Policies and Procedures:** Define clear policies and procedures for acquiring, deploying, managing, and disposing of your assets.
2. **Asset Discovery:** If you don’t have many assets, the discovery process can be as simple as walking around your facility and recording asset details on paper. Automated tools can make asset discovery more efficient, particularly when gathering details about IT and OT assets is too difficult to do by hand.
3. **Asset Classification:** Categorise your assets based on their type, criticality, and sensitivity.
4. **Asset Tagging:** Track your assets by assigning unique identifiers (e.g., asset tags). This can be done simply and cheaply with stickers and markers or through use of electronic tagging and tracking solutions.

5 **Lifecycle Management:** Implement processes for managing each stage of the asset lifecycle, including procurement, deployment, maintenance, upgrades, and disposal.

6 **Software License Management:** Track your software licenses to ensure compliance with vendor agreements and avoid overspending.

7 **Maintenance and Support:** Maintain records of your maintenance activities, support contracts, and warranty information.

8 **Audits:** Conduct regular audits to verify the accuracy of your asset inventory. Identify and correct any discrepancies.

9 **Reporting and Analysis:** Generate reports on your asset inventory, usage, and lifecycle status with a frequency that allows you and your management to take action in a timely manner if required.

10 **Continuous Improvement:** Regularly review and update your asset management processes to ensure they remain effective.

Skills for an Asset Management Team

Having the right people with the right skills for asset management ensures accurate data collection and analysis, effective implementation of processes, and the ability to leverage data for informed decision-making across your organisation. This ultimately maximises the return on investment in IT, OT, people, and data assets and minimises security risks. Crucial know-how includes:

- **Enterprise Knowledge:** Knowing where your physical and virtual assets are located.
- **Analytic Skills:** Ability to collect, organise, and analyse asset information.
- **Communication Skills:** Ability to communicate effectively with your staff. Involve them in identifying, tagging, and managing assets.

Maintaining an Asset Management Program

Maintaining an asset management program requires your attention because your technology environment is constantly evolving. New technologies, threats, and business needs require regular reviews and updates to ensure your program remains relevant and effective, and continues to provide accurate data for security and business decisions. To be successful you must:

- Identify and track key metrics to measure the effectiveness of your asset management program over time.
- Periodically review and update asset management policies and processes.
- If conditions and circumstances allow, consider automating asset discovery, tracking, and reporting.
- Provide regular training about asset management to all staff so they understand the importance of supporting your program.

Failing to maintain the program leads to data decay, inaccurate inventories, and a diminished ability to manage risk or optimise IT spending. Asset management programs do not come without a cost, but you can extract more value out of your asset inventory and potentially recoup or at least offset some of those costs if you integrate your asset management with other IT or security initiatives, such as CMDB or Security Information and Event Management (SIEM).

How Asset Management Supports Cybersecurity

The first principle behind all cybersecurity efforts is to know what you are protecting. This is why asset management is so important when it comes to reducing risk and countering threats. That includes:

- **Vulnerability Management:** Accurate asset inventory is crucial for identifying and prioritising vulnerabilities.
- **Incident Response:** Asset management data helps incident responders quickly identify affected systems and their dependencies.
- **Security Audits:** Asset management provides the evidence needed to demonstrate compliance during security audits.
- **Software License Compliance:** Proper software license management reduces the risk of using unlicensed software, which can introduce security vulnerabilities.
- **Endpoint Security:** Asset management helps organisations track and manage all endpoints, including laptops, mobile devices, and IoT devices, ensuring they are secured.

Asset management is the cornerstone of a strong cybersecurity program. By effectively managing your assets, your organisation can significantly reduce security risks, improve compliance, and optimise resource allocation. A well-implemented asset management program is an investment that pays dividends in enhanced security and business resilience.

Further Guidance

1. NIST Cybersecurity Framework: **ID.AM: Asset Management - CSF Tools**
2. UK National Cyber Security Agency (NCSC) guidance: **Asset management - NCSC.GOV.UK**
3. ENISA guidance: **WP2016 1-2 2-1 Hardware Threat Landscape and Good Practice Guide.pdf**
4. UK High Value Manufacturing Catapult guidance: **HVMC_Cyber-Security-Report_Full.pdf**

SUPPLIER COMMUNICATION | Rolls-Royce's **Global Supplier Portal** is your first stop for information and documents, such as Notices to Suppliers (NTS).