Industry White Paper

Hardware and Software Asset Management: Asset Management as a Security Initiative

Closed Loop Lifecycle Planning©
In collaboration with HP®, Microsoft®, and Intel®

April 2025

Submitted by: Jeff Malec, HP Principal Technologist and Lifecycle Subject Matter Expert
Bruce Michelson, Distinguished Technologist Emeritus HP
Close Loop LLC, Manager

Table of Contents

About the Authors

Jeff Malec

Jeff Malec is an HP Principal Technologist and Lifecycle Planning Subject Matter Expert. After a 21+ year career with Microsoft, Jeff joined HP and is driving adoption of the modern workplace, Windows 11, and the related lifecycle elements.

Managing the Microsoft and HP relationship for several years, Jeff is an expert in go to market plans and customer adoption strategies.

Jeff holds multiple technical certifications from Microsoft.

Bruce Michelson

Bruce Michelson is an HP Distinguished Technologist (Emeritus) and the Manager of Close Loop LLC. Bruce has over 36+ years in delivering industry white paper and customer engagements. Bruce has delivered over 1,000+ white papers and over 350+ engagements.

Bruce is the author of seven books regarding aspects of lifecycle management. Bruce has numerous copyrights and patents regarding his expertise in User Segmentation, lifecycle management, cost of change, The Ready State©, and Appropriate Incumbent Behavior©.

Bruce teaches IT in Health Care and Advanced Systems and Design at Florida Atlantic University where he is an adjunct.

Bruce is sponsored by the HP, Microsoft, and Intel Alliance for this engagement.

1.0 Management Summary

Hardware and Software Asset Management is a familiar topic to our readers. Organizations have been engaged on these lifecycle elements since the very beginning of client computing.

Asset management has had a varied reputation. The value it brings has not been well documented or promoted as an added benefit, but rather as a necessity due to directives. Over time, results have differed based on the maturity of the organization and various practice levels. Some organizations have reported having good control during acquisition and disposal of equipment but lacking discipline in the interim stages. Another common observation is that software controls can be too complex or insufficient in managing user privileges for loading applications from the internet.

During the pandemic, the importance of remote work procedures and the provision of appropriate hardware and software portfolios became increasingly relevant. Moreover, security issues gained significant attention, particularly in relation to remote and work-from-home users targeted by malicious actors.

As we transition into the post-pandemic era, cybersecurity has become a paramount concern and is now the primary KPI for most organizations. It is no longer sufficient to merely manage assets adequately; organizations must adopt advanced practices to safeguard their operations, end users, and customers. Phishing remains a prevalent threat, primarily involving endpoint devices and their users.

Today's organizations must accurately identify not only the location of each device but also the contents stored on those devices. If this information is unknown, it is often presumed that personally identifiable information (PII) or other sensitive data may be at risk.

Effective asset management for hardware and software is a fundamental building block of security. Without advanced practices, many questions regarding security, exposure, and risk remain unanswered.

2.1 What are the Rules?

Regardless of the industry focus, there are federal, state, local, and industry regulations regarding security that represent a baseline for an organization. Financial statements and other filings require the acknowledgement of certain counter measures and strategies.

1.2 Legacy – IT Orientation

Hardware and Software Asset Management have typically been considered and perhaps remain, IT-centric functions. In previous years, budgeting and funding for asset management was a challenge to obtain as outcomes were often considered “soft costs.”

From an operational and technical perspective, asset management is deployed by IT. However, just as we have stated that “Windows 11 as a security initiative delivered by IT”, one can leverage that same logic in stating that the “hardware and software asset management is a security initiative delivered by IT.”

Breaking the legacy perspective of asset management is fundamental given the impact of the trends in the industry such as AI, modern management, and personas.

Asset management enables the foundation of the security strategy. In order to secure a device and protect end users, organizations need to know the device location, device contents, and how exposure can be mitigated based on the prior two pieces of information.

1.3 Objectives of This White Paper

This White Paper aims to offer insights into hardware and software asset management. It urges organizations to enhance their practices to mitigate risks associated with lower practice levels.

2.1 Potential Role of the Service Desk

The service desk, also referred to as a help desk, can add significant value to asset management. Service desks now have mature capabilities for data analytics before and after incidents.

An organization typically has 80% of its end users contact the service desk monthly. Using service desk data helps determine the exact figure.

Regardless of the figure, contacting the help desk allows the organization to perform a "cycle count" of the end user's hardware and software. This is similar to a traditional "cycle account" but can be done in real-time.

Similar information can also be obtained from data analytics management tools, which can either be standalone or integrated into the service desk data.

The key point is that modern IT provides an opportunity to update asset management repositories without disrupting or affecting end users.

As AI becomes more prevalent, it will serve as an additional vector in asset management discussions to derive insights regarding the state of asset management practices.

2.0 Hardware Asset Management

One might assume that hardware asset management is straightforward; however, it is complicated by the various roles and responsibilities of end users.

First, let us consider the common elements that all organizations can access and record in a hardware asset management repository. Below are logical points for capturing hardware information:

- Acquisition or point of sale information which would include date of birth, asset tag, serial number
- Configuration information such as peripheral and components (disk, memory, chipsets, camera, mice, keyboards)
- Bill-to, ship-to, sold-to information
- Pre-deployment location
- Deployment information (from asset tag or serial number)
- Device registration end user name, location, date of deployment
- Warranty commencement date

- End of life date, decommissioning
- Disposition

These processes are managed through an asset manager tool such as SCCM, Intune, or other third-party tools.

With the increasing variety of mobile products, more devices may be offline or out-of-band at certain times. Asset management can still occur with lifecycle elements including solutions like Intel vPro or HP Protect and Trace, and other third-party solutions.

Every time a system is accessed, whether desk-side or virtual, it should be considered a cycle count and compared to the repository of record.

2.1 Mobility

For years, there have been varying definitions for mobility. One definition focused on laptops as the primary use case for mobility. Concurrently, another definition of mobility centered on cellular technology, with tablets falling somewhere in between.

Many organizations have allocated different resources and teams to these technologies, believing that the differences warranted such separation. However, there is an argument against this approach - the end users utilize both or all three types of technologies. The separation was based more on IT's perspective of what they were willing to provide, rather than considering what the end users actually use. This division has led to increased costs, less efficient resource utilization, and impacted the end user experience.

The separation was partly due to the differences in tools, form factors, and suppliers. However, the assumption was that multiple organizations and specialized teams were necessary. Skills were considered highly specialized and non-transferable. While this might have been true historically, these portfolios are now commoditized and should be rationalized. Despite having different suppliers, the roles and operations are quite similar, including asset management and security. Therefore, these technologies should no longer be separated when considering mobility.

2.2 Practice Levels

The practice levels for hardware asset management are determined by the integration of various sources that can confirm the status of the asset. Higher practice levels have solutions capable of tracking assets when they are lost, stolen, or missing.

Many devices go missing every month according to statistics. The higher the practice level, the greater the ability to identify, locate, and remediate (either identify or disable the device).

Real-time data analytics should contribute to the hardware asset management repository to ensure consistency with overall solutions – there should be a single source of truth in asset management.

Each contributing system and process must be accurate.

3.0 Software Asset Management

Unlike hardware asset management, software asset management requires a different discipline and unique skill sets. Instead of focusing on asset tags and serial numbers, it involves capturing a comprehensive set of empirical data to achieve advanced practice levels.

Closed Loop Lifecycle Planning has developed a methodology known as "Software Rationalization." This approach aims to identify all software within the installed base and categorize it based on predefined criteria, determining what is core and non-core to the organization.

Unlike hardware asset management, software asset management relies on different foundational criteria. The security of an organization depends on a baseline of actions associated with software business practices.

The elements of software asset management are designed to assess and provide counter measures through governance and processes to avoid security issues associated with software. The following are some of the elements that are a part of the software hardware asset foundation:

- *Software In-Take*
  Assurance that net new software is fully vetted and approved.
- *Software Ownership*
  Assurance that all software that resides in an organization's installed base has a defined software owner responsible with a description of precisely what software ownership encompasses.
- *Version control*
  Older versions of software are less secure than its current counterparts. Adherence to best practices regarding software version control represents a security vector.
- *Administrative Privileges*
  Many organizations still struggle with providing on-going privileges to certain end users for downloading, accessing, or somehow acquiring net new software. From a security perspective, this permission a potential source of adware, malware, and other cyber-exposure. Most end users are not security experts, so the due diligence is often performed after the software is acquired. Most downloads require approving the terms and conditions which most end users are not authorized to sign.
- *Software Usage*
  The actual use of software is a security issue. Having software reside in an installed base, unused, could be a source of cyber-exposure since it is likely that no one is accountable for its presence.
- *Software Updates, Packaging, and Patching*
  Recent developments (such as Blue Screen Friday) provided a real-world example of the implications of not fully vetting and assessing the on-going required support of installed base software. This is now a security issue; it always has been but often it takes an issue to highlight the gap in practice levels.

The point of this section is to highlight that software asset practice is not only one element, but also the aggregation of all of the elements into a practice. While the operational aspect will always remain with IT to technically deploy all of the solutions, it is security that should own the adherence to policy, process, procedure and governance.

3.1 Practice Levels

The hardware asset management practice is an essential part of an organization's security. Older legacy applications, which represent technical debt, can pose security risks, while others may be managed by IT rather than security.

Closed Loop Lifecycle Planning suggests that ownership of the software asset management practice should reside with security, while IT handles execution. Historically, IT has enforced compliance for both software and hardware. However, since security is the core concern in this context, it may be more effective for security to own the planning, design, and compliance aspects of software and hardware asset management.

With cyberattacks being common today, it is important for security teams to take primary responsibility for these practices. Expecting different outcomes without changing ownership structure may not be reasonable. Cyber security should be central to the strategy and the responsible entity.

4.0 CMDB and Asset Management Relationship

Many organizations consider the development and ongoing support of the CMDB as the single source of truth in the organization. Based on frameworks and advanced best practices, this could be considered a reasonable assumption. However, very few organizations have achieved the advanced best practice levels necessary for the CMDB to deliver that role effectively.

From an academic perspective, the vision is accurate, but operationally, there are factors to consider. As the central repository, the CMDB relies on the integrity of its information. The phrase "garbage in, garbage out" highlights the importance of data accuracy. For the CMDB to function as a single source of truth, all data within it must be fully accurate, not just 70% to 80% accurate.

Organizations may sometimes cite timing as the reason for data gaps, but leaders and security personnel may perceive this as non-compliance and inaccuracy rather than a timing issue. Accurate hardware and software asset management, along with enforced governance, are essential for the reliability of the CMDB. If the supporting asset management feeds are not fully accurate, the CMDB will not be reliable.

Adding to the complexity, the CMDB includes many possible sources of information. If the gaps are noticeable, the CMDB may not be viewed as valid. From a security perspective, if the CMDB cannot be trusted, it becomes a security issue rather than an IT issue, as outcomes and strategies might be based on flawed data.

4.1 Practice Levels

The data fed into the Configuration Management Database (CMDB) must be at an advanced practice level before inclusion. Migrating inaccurate or improperly formatted information into the CMDB necessitates re-architecting entire workflows and solutions—a basic IT premise to be avoided.

In many organizations, the CMDB has been treated as a "catch-all" project, serving merely as a centralized repository for all IT-related and end-user information. The initial focus was on populating the CMDBs, with accuracy addressed at a later stage.

Maintaining an inaccurate database, regardless of the intention, leads to confusion and concern. This underscores the fundamental difference between IT-driven strategies for populating databases and creating secure and accurate repositories.

Security prioritizes the accuracy of data feeds before workflows are established. Conversely, IT often focuses on the establishment of new repositories. This discrepancy results from the ownership of repositories being aligned more with implementers than with planners and designers.

While this may be a timing issue, it illustrates that ownership of the process encompasses both security and operational concerns. In many organizations, this process has inadvertently been reversed.

5.0 Relationship Between Governance and Asset Management

Asset management requires effective and contemporary governance. Previous generations of governance did not anticipate all the changes to the current environment. Security must now be proactive.

Trends in mobility, cyberattacks, AI, NPUs, the cloud, along with consumerization trends that have matured since the pandemic, are driving the need for new governance to address emerging threats.

Hardware and software asset management continue to be somewhat traditional in their structure and focus. As foundational elements, there are new types of asset management approaches such as geo-fencing, remote wipe, and out-of-band remediation. These new technologies require governance, and their implementation within an organization should be driven by security considerations.

5.1 Future Proofing

Future proofing infrastructure necessitates a comprehensive review of hardware and software asset management practices within an organization. This is not only crucial for identification purposes but also to ascertain the required security countermeasures.

The level of detail in asset management must be reevaluated through the lens of a risk assessment. Applications previously considered routine, such as collaboration tools, now bear new elements of risk and compliance.

The emergence of artificial intelligence introduces different risk factors. Endpoints will increasingly become targets for malicious activity, more so than they are currently. Furthermore, end users will play a significant role in actions leading to cyberattacks, with phishing already being a predominant cause.

5.2 Audits

The role of audits in identifying practice levels, risk, gaps, and interfaces in asset management (including the CMBD) should be significantly expanded in terms of both frequency and scope.

Audits should be conducted independently, both externally and internally. Rather than limiting audits to an annual basis, it is necessary to perform cyclical or periodic assessments, with more frequent processes such as bi-annual or quarterly audits. This clearly represents an investment opportunity.

Moreover, new management and security tools can assist in identifying emerging risk vectors and rationalizing legacy systems, whether through updates or replacements. This process should be considered an ongoing requirement.

7.0 Observations and Conclusions

Closed Loop Lifecycle Planning has found, “there are no right or wrong answers, only conscious and unconscious decisions.”

The choice to maintain the traditional approach to hardware and software asset management is one of these decisions.

This next generation of technologies should prompt a new organizational perspective on roles and responsibilities.

As mentioned in this White Paper, the skill sets for hardware and software asset management should be reconsidered. There are business requirements, technological requirements, and a forward-looking view of exposure.

Based on the number of cyberattacks so far and those anticipated in the future, continuing along the current path will not change outcomes.

The conclusion of this White Paper is clear - *the foundation of security must be solid, and hardware and software asset management must reach advanced practice levels to be effective*.

Appendix

1. Closed Loop Lifecycle Planning - A Complete Guide to Managing Your PC Fleet, Bruce Michelson, published by Addison-Wesley Division of Pearson Education, ISBN 978-0-321-47714-9.
2. Appropriate Incumbent Behavior©, copyright Bruce Michelson.

Other Books by Bruce Michelson

1. Closed Loop Lifecycle Planning©, Client Computing in the Health Care Industry, by Bruce Michelson, Published by IDG, ISBN 978-1-61623-045-6.

2. Closed Loop Lifecycle Planning© - What It Is and Why It Is Important to You, by Bruce Michelson, Published by Bookmasters, ISBN 0-9667607-0-0.

3. We Are All Retail, The Race to Improve the Retail Experience in a Post Covid World, by Bruce Michelson and Leif Olson, Published by Archway Publishing, ISBN 978-1-6657-3394-6.

4. IT Strategies in the Post-Pandemic Era, Part of the Closed Loop Lifecycle Planning© Series, published by Archway Publishing, March 2023, ISBN 978-1-6647-3856-9.

5. Zero Trust, by Bruce Michelson and Cody Gerhardt, published by Archway Publishing, May 2023, ISBN 978-1-6657-4191-0.