END-OF-LIFE (EOL) MANAGEMENT

What are end-of-life (EOL) assets?

End-of-life (EOL) assets are retired software or hardware assets that no longer receive updates or security patches from their vendors, making them attractive and frequently compromised targets for cyber criminals.

Why is EOL management so important for the institution?

The modern financial institution is increasingly dependent on technology to perform a host of tasks, ranging from applications that enable the most mundane of daily operations to the core platform systems that are the very lifeblood of the institution's operations. Yet, as this beneficial technology has increasingly become integrated into our institutions, so has the need increased for effective **life cycle management of technology assets**. Institutions commonly maintain patch management programs to handle ongoing maintenance and updating of hardware and software assets. However, these same hardware and software assets generally have limited life spans and, because updates and security patches are generally not provided (without special arrangements) once these assets are retired by their vendors, they become attractive and frequently compromised points of entry for cyber criminals. For this reason, **it is vitally important that every institution maintains a program to identify and manage EOL assets and the associated risks as part of the larger asset life cycle management program.** The institution simply cannot manage or apply adequate security protections to assets it does not know it has.

Financial institutions often find comfort in the reliability and convenience of the technology tools that enable their everyday business operations. Moreover, financial considerations and the costs of implementing and integrating new technology can further increase disdain on moving away from outdated or unsupported technology. However, there are several important reasons why EOL management is so critical for financial institutions. Inadequate management of EOL hardware and software assets and relying on outdated or unsupported technology can create:

- **Exploitable vulnerabilities**. Unpatched or outdated technology opens the door to easily exploitable and frequently targeted vulnerabilities, which can lead to unauthorized access to information, data breaches, and the introduction of malware.
- **Compatibility issues**. Leaving EOL assets or outdated technology in the environment may lead to compatibility issues with other technologies in the institution. Future upgrades or replacements of other technologies may conflict with unsupported legacy hardware and software, creating conflicts, limiting modernization efforts or affecting usability and security of existing technologies.
- **Increased costs.** Unsupported technology can lead to Increased costs associated with maintaining outdated software, addressing usability conflicts, and potential reductions in system performance, security, or reliability.[1]

Clearly, the risks and potential costs of maintaining outdated and unsupported hardware and software assets far outweigh any benefits of relying on unsupported technologies. But getting a handle on the management of outdated hardware and software assets is an ongoing process that requires a clear view

[1] Todd, H. (Yorb). *The Consequences of Ignoring End-of-Life Systems and Hardware,* July 31, 2023.

of all the institution's assets and an understanding of the interdependencies that exist between outdated assets and other institution systems.

Understanding the EOL management process

Management of EOL assets requires a forward-thinking approach, as replacing hardware and software assets generally requires awareness, time, and planning. This can create significant impacts on the operation of other systems in the institution and is rarely accomplished smoothly and without disruption in the absence of a comprehensive plan for replacement.

According to the FFIEC IT Handbook booklet: *Information Security*, "Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers." In addition, support from any third-party system vendors and the risks associated with operating unsupported legacy systems should be included in the institution's life cycle management strategy.[2] The FFIEC notes that effective EOL management should include the following:

- Maintaining inventories of systems and applications.
- Adhering to an approved end-of-life or sunset policy for older systems.
- Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor.
- Conducting risk assessments on systems and applications to help determine end-of-life.
- Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications.
- Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information.[3]

Compensating controls

There may be instances where EOL systems must temporarily remain within the institution due to compatibility issues, special financial considerations, etc. In these cases, it is essential that compensating controls exist to mitigate the associated risk. These controls may include isolating or segregating the unsupported asset from the network, adjusting existing security configurations, and/or acquiring extended support and service contracts from the vendor, when available. According to the FFIEC, "Management should also have a plan to replace the system or application and implement compensating controls until replacement. Strategies for replacing and updating hardware and software should incorporate and align with overall information security and business strategies as appropriate."[4] Ongoing tracking of any unremediated EOL hardware or software assets can help ensure they are managed in accordance with the institution's risk acceptance policy and established risk tolerances prior to replacement.

---

[2] FFIEC. *FFIEC Information Technology Examination Handbook: Information Security - II.C.11 End-of-Life Management,* September 2016.
[3] Ibid.
[4] Ibid.