MORETON & COMPANY

MUNICIPAL **INSIGHTS**

A Moreton & Company Public Entities Newsletter

Cyber Risks & Liabilities

Managing End-of-Life Software

At some point, all software will reach the end of its life. Manufacturers will no longer develop or service the product, discontinuing all technical support, upgrades, bug fixes, and security fixes. As a result, end-of-life (EOL) software will have known vulnerabilities that cybercriminals can easily exploit. This article discusses the risks of continuing to use EOL software and best practices for organizations to mitigate this risk.

Risks of EOL

Known but unmitigated vulnerabilities are among the highest cybersecurity risks. One survey found that 60% of data breaches stemmed from unpatched known vulnerabilities. Another report found that 3 of 4 cyber-attacks in 2020 exploited security vulnerabilities from 2017 or earlier.

Organizations may be hesitant to transition away from EOL software for a number of reasons, such as:

- New software lacks the necessary features
- Limited resources
- Migration challenges
- Lack of accountability for replacing software

This is especially true when EOL systems are still functioning. However, continuing to use EOL software also comes with a myriad of risks, such as the following:

- **Heightened cybersecurity risk.** Without security fixes from the developer, EOL software becomes riddled with security hazards that hackers are often quick to exploit.
- **Software incompatibility.** New applications will be designed for current software, meaning EOL software is often unable to accommodate newer apps. Organizations that continue to use EOL software will likely have to hold onto legacy systems and applications, even when newer and better versions become available. This poses additional risks, as out-of-date applications may soon reach EOL as well.

"It's evident that EOL software exposes organizations to heightened levels of risk...

...Through proper planning and device management, businesses can stay sufficiently protected against these known cyber vulnerabilities."

- **Inability to remain compliant.** Regulations requiring companies to meet minimum data security standards are on the rise. As a result, organizations that use EOL software and fail to adequately protect sensitive customer data may be deemed non-compliant. Consequences may include fines or company shutdowns.
- **Increased operating costs.** Attempting to maintain, patch, and bug-fix EOL software without developer assistance can be costly. In some cases, the cost of trying to patch EOL software may exceed that of replacing old software, to begin with.
- **Poor performance & reliability issues.** If your organization is running out-of-date software, there is an increased likelihood that your software or systems could break down. Such failures can result in costly downtime and additional operating costs.

Proactive management is a necessary step to prevent unwelcome surprises and keep your organization secure.

Managing EOL Software

Although many organizations are prepared for the initial life cycle stages that come with introducing new products, few businesses prepare for what will happen when it inevitably comes time for these software components to be phased out. Consider the following tips for EOL management:

- **Create a life cycle management plan.** Effective planning for EOL reduces cybersecurity vulnerabilities, lessens the risk of downtime, and helps companies remain compliant with regulations. Your life cycle management plan should include all aspects of a product life cycle, beginning with the introduction of new software to EOL and extending to plans for phasing out unsupported software.
- **Understand your device history.** Use device management software that will automatically capture important information about devices when they connect with the network (e.g., model number, IP address, certificate status). Such software can provide your organization with a highly detailed network overview and will enable your organization to push software and firmware updates, certifications, and other necessary upgrades to thousands of computers on your network simultaneously.
- **Monitor status.** Stay current on EOL notifications regarding critical components of your entire organization. Most major suppliers have life cycles for products and their components, including EOL dates. Best practices suggest reviewing the EOL dates of new software before selecting it for current use. Planning for EOL will help your organization avoid any surprises about when devices or software will no longer be supported, enabling your organization to plan and budget for the replacements.
- **Maintain consistent cybersecurity practices.** To ensure compliance with cybersecurity best practices, consider policies surrounding changing default passwords, password strength, compliance with regulations (e.g., Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard, and National Defense Authorization Act), and how frequently risk levels are assessed.
- **Communicate early & clearly.** Inform customers of all upcoming EOL issues and your plans for addressing them. Being communicative and transparent can help your organization improve customer loyalty and trust during EOL transitions.

Conclusion

It's evident that EOL software exposes organizations to heightened levels of risk. Additionally, many insurers will ask for information on EOL management as a prerequisite to obtaining cyber insurance. Through proper planning and device management, businesses can stay sufficiently protected against these known cyber vulnerabilities.

For more risk management guidance, contact a member of Moreton & Company's Public Entity Team.

Please visit www.moreton.com/news-events/ for more information and to view other newsletters. For additional questions, please contact your Moreton & Company representative.