# Cyber-risks & Liabilities

Courtesy of The Risk Hub Ltd

## Managing End-of-Life Software

At some point, all software will reach the end of its life. This means manufacturers will no longer develop or service the product, discontinuing all technical support, upgrades, bug fixes and security updates. As a result, end-of-life (EOL) software will have known vulnerabilities that cyber-criminals can easily exploit. This article discusses the risks of continuing to use EOL software and outlines best practices organisations can implement to help mitigate these concerns.

### Risks of EOL Software

Known but unmitigated vulnerabilities are among the highest cyber-security risks. In fact, a survey by software company Tripwire found that 1 in 3 (34%) European organisations have experienced security breaches due to unpatched vulnerabilities. Furthermore, a recent government cyber-security survey revealed that 63% of UK businesses lack robust vulnerability management policies, thus leaving them increasingly exposed to digital threats.

Despite these findings, organisations may be hesitant to transition away from EOL software for a number of reasons, such as:

- **An absence of necessary features in new software**
- **Limited resources**
- **Migration challenges**
- **A lack of accountability for replacing software**

In addition to these reasons, organisations could be particularly apprehensive of leaving EOL software behind if such systems are still functioning. However, continuing to use EOL software also comes with a myriad of risks, such as the following:

- **Heightened cyber-security risks—**Without security fixes from developers, EOL software can become riddled with vulnerabilities that hackers are often quick to exploit.
- **Software incompatibilities—**The latest applications are designed for current software, meaning EOL software will likely be unable to accommodate newer technology. As such, organisations that continue to use EOL software may 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 This poses additional risks, as out-of-date applications may soon reach EOL status as well.
- **Compliance concerns—**Certain regulations require companies to meet minimum data security standards. As a result, organisations that use EOL software and fail to adequately protect sensitive customer data may be deemed non-compliant. Consequences may include fines and reputational damage.
- **Increased operating costs—**Attempting to maintain, patch and fix bugs in EOL software without developer assistance

can be expensive. In some cases, the cost of trying to patch EOL software may exceed that of replacing the technology altogether.

- **Performance and reliability issues—**Organisations running out-of-date software may be more likely to experience system breakdowns. Such failures can result in costly downtime and additional operating expenses.

Considering these risks, proactive EOL software management is necessary for organisations to prevent unwelcome surprises and keep their operations secure.

## Managing EOL Software

Although many organisations are prepared for the initial steps that come with introducing new software, few businesses are prepared for what will happen when it inevitably comes time for these systems to be phased out. With this in mind, organisations should consider the following EOL software management tips:

- **Create a lifecycle management plan.** Effective planning for EOL software can reduce cyber-security vulnerabilities, lessen the risk of downtime and help companies remain compliant with applicable regulations. A lifecycle management plan should include all aspects of a product's lifecycle, beginning with the introduction of new software and extending to procedures for phasing out unsupported software.
- **Understand device history.** Organisations should use device management software that will automatically capture important information about devices when they connect to a network (eg model number, IP address, certificate status). Such software can provide organisations with highly detailed network overviews and enable them to push software and firmware updates, certifications and other necessary upgrades to thousands of computers on their networks simultaneously.
- **Monitor EOL status.** Organisations should also stay current on EOL notifications for all critical workplace systems. Most major suppliers have set lifecycles for products and components, including EOL dates. Best practices suggest reviewing the EOL dates of new software before selecting it for current use. Planning for EOL dates will help organisations avoid any surprises regarding when software will no longer be supported, enabling them to budget for replacements.
- **Maintain consistent cyber-security practices.** Effective cyber-security practices can also help organisations ensure proper EOL software management. Some areas for organisations to consider include policies surrounding multi-factor authentication, password strength, compliance with applicable regulations (eg the General Data Protection Regulation and the Data Protection Act 2018) and the frequency of risk assessments.
- **Communicate early and clearly.** Organisations should inform customers of all upcoming EOL issues and outline their plans for addressing these concerns. Being communicative and transparent can help organisations improve customer loyalty and trust during EOL transitions.

## Conclusion

It's evident that EOL software can expose organisations to significant cyber-security issues. Additionally, many insurers will ask organisations for information on EOL software management as a prerequisite to providing cyber-insurance. However, through proper planning, organisations can stay sufficiently protected against these known software vulnerabilities. Contact us today for further risk management guidance.