HOW TECHNOLOGY REACHING END OF SERVICE CAN IMPACT YOUR BUSINESS

Supported technologies have routine internal security measures in place while their support teams create and release updates and patches to make the product more secure and helpful. When your organization's software reaches End of Life (EoL) or End of Support (EoS), it will no longer receive critical updates and patches even though it may still function. This can have dangerous repercussions for your business. To save money, some business owners may resist upgrading to next-gen hardware and software. However, the results are pricey in more ways than one. Utilizing software after its "best by" date puts your business at risk for security breaches. The bottom line is that employing EoL technology puts the security, performance, compliance and compatibility of your IT infrastructure in danger.

4 MAJOR RISKS THAT EOS TECHNOLOGY POSES TO YOUR BUSINESS

SECURITY RISKS
Security patches and updates keep your business network secure against vulnerabilities that hackers may exploit. However, if you're using EoS software and hardware that can no longer support these critical patches and updates, hackers can easily take advantage of the vulnerabilities and infiltrate your network. The risk of ransomware via EoL software extends beyond downtime to reputational damage, customer churn and revenue loss.

PERFORMANCE ISSUES
Older hardware and software are more likely to malfunction, fail and have problems. This can frequently cause delays and interruptions in your business operations, giving the impression that you are unreliable, which can possibly cost you clients. When you have up-to-date hardware and software solutions, you have the highest level of reliability, in turn improving your brand.

COMPATIBILITY CONCERNS
Your software will typically continue to operate as intended when support ends — until it doesn't. Instability and incompatibility issues could ultimately make the software unusable. EoS deprives IT departments of manufacturer support, forcing them to buy new software before they have an upgrade strategy. Additionally, if you're using EoL operating systems, you may have to stick with outdated software since operating systems are optimized for new apps.

COMPLIANCE RISKS
It's more difficult and expensive to follow government and business requirements when using older technologies. Entrusting your important data to an insecure application or an OS that has reached the end of its useful life may lead to hefty fines, business closures or even potential jail time. By doing this, you jeopardize not only the privacy of your customers but also your legal standing. The effects could be catastrophic for your customers and your business.

It may be very challenging to keep up with evolving technology, given the amount of infrastructure that most businesses need. Partnering with an IT service provider is the simplest way to ensure all your hardware and software are regularly maintained and upgraded. Keeping your technology up to date is simple once you have a trusted advisor like us in your corner.