# Discussing Windows® XP Migration with Management– The Top 5 Threats to Business

## The need to migrate from soon-to-be-obsolete Windows XP in terms that a non-technical business manager/executive can understand

When Windows XP was first launched on October 25, 2001, it represented a highly anticipated and desirable upgrade to Windows® 98 and other previous versions. It became the cornerstone of end-user computing, bringing new technologies and improved usability. According to Net Applications,

**Windows XP was the most common operating system in use until Windows 7 overtook it in August 2012.**

CONTENTS

**Using Windows XP after** its formal "end of life" on **April 8, 2014 creates a number of potentially serious problems** for the organization.

With its major security, management, and interface limitations, **Microsoft has decided to end support for Windows XP**. This decision has important implications for corporate management as **it presents a number of risk, security, operations and compliance issues** that will be detailed in this white paper. Simply put, using Windows XP after its formal "end of life" (EOL) on April 8, 2014 creates a number of potentially serious problems for the organization. This white paper will look at the **top 5 issues that business management must be aware of** and the impact that a specific issue has on the organization from a non-technical perspective. It will give you the business justifications for driving a migration program forward by providing more understanding of the importance and implications of this issue in their language.

## How Windows XP's EOL Can Negatively Impact an Organization

Technology's role is to enable the organization to deliver better business results. However, problems with technology can negatively impact these results, and this is the fear when it comes to the end of life for Windows XP.

### 1. Known Security Vulnerabilities Will Not Be Fixed

The most important technical issue from Windows XP's EOL is that the automatic delivery of free security patches to fix known vulnerabilities will not be available. This is effectively like telling burglars where you've hidden your spare keys.

These patches are generally delivered regularly on what is known as "Patch Tuesday," when Microsoft details the issue and then provides the patch to fix it. It is likely that within a few short weeks of its end of life, **hackers will exploit new vulnerabilities in Windows XP** to gain entry into IT infrastructure. Reports from analysts that follow the hacker community indicate that some professional hackers are waiting for the EOL date and are planning attacks soon after. These hackers will be taking advantage of the "open door" to your IT environment.

**The most important technical issue** from Windows XP's EOL **is that the automatic delivery of free security patches** to fix known vulnerabilities **will not be available.**

Organizations can continue to receive patches, but have to meet certain criteria and pay a substantial yearly fee. Individual Microsoft Premier customers with large numbers of PCs have told *Computerworld* that these fees range from $600,000 to $5 million *for the first year.* **Microsoft has indicated that this fee will increase in subsequent years.**

### 2. Potential Legal Liabilities

Arguably the most important potential vulnerability that Windows XP will present to organizations after its EOL is that its continued use may result in legal entanglements. There has been a tremendous amount of recent legislation and development of statutes focused on the consequences of data theft and exposure

The continued use of Windows XP **may result in legal entanglements.**

when corporate systems are compromised. Governments have responded to a flood of breaches by enacting laws that add clarity to what the minimum acceptable requirements are to secure personal and private information.

Among the clearest statutes that document the government requirement for protection of private information is the United Kingdom's Privacy Act. The reason that this statute is important is that **it explicitly calls out the need to have "modern and up- to-date" software** to protect private information. Clearly, Windows XP will not meet that standard after the EOL date. Organizations using Windows XP conducting business in the UK face potential legal liabilities if a breach originates from one of their PCs.

In the United States there is quite a bit more complexity, as there are many differing statutes focused on data protection and privacy. States have the latitude to enact their own standards, so there is substantial variation. However, one of the most common elements that impacts liability for data loss is the concept of "reasonableness." In other words, what is a reasonable and prudent set of actions to protect someone's private information and data? This is where Windows XP presents a very real potential vulnerability. Given the level of media attention and the amount of focused information, **leaving such systems in place may not be perceived as a "reasonable" thing to do.**

Further, with the specific threats that have been outlined in the press and in documents focused on the Windows XP user, including this one, **some lawyers postulate that leaving these systems in use would constitute negligence** on the part of the organization. Even though the Microsoft Custom Support Agreement will continue to provide operating system patches, there are known threats from other aspects of Windows XP, including the lack of support from third-party security tools.

**It's not just Microsoft** that is going to end the life of Windows XP.

## 3. Key Security And Software Vendors Are Also Ending Support For Windows XP

The security tools and software needed to protect PCs against threats come from a large number of vendors. Starting with an evaluation of endpoint security (anti-virus, anti-malware, etc.) products, the trend is clear. Research firm TechTarget has reported that **it is likely that key security software vendors such as Symantec, McAfee, and Trend Micro will also cease or dramatically cut back their support for Windows XP,** as the product will effectively be "dead." Existing software may run, but without the updated virus signatures and technology to stop the latest threats, **Windows XP systems may end up effectively "defenseless."**

However, it is important to realize that security requires much more than endpoint protection, and much like the case for endpoint security, it's likely that Windows XP support will fade quickly for tools like mobile device management (MDM), identity management, virtual private networks (VPNs), Public Key Infrastructure (PKI) management, and more. These vendors face much of the same decision processes, as they realize that

Windows XP is a "dead" operating system and that inconsistent patching makes working with it even more complex. This scenario results in high costs and very little revenue, making abandonment an easy decision.

One specific area that may be affected very quickly is MDM, which insures that PCs or devices connecting to your network have up-to-date security credentials. After Windows XP's EOL, those systems will no longer be able to show current credentials.

Simply put, **it's not just Microsoft that is going to end the life of Windows XP.** Literally hundreds of other vendors can no longer justify the resources and costs to support an obsolete operating system. It boils down to a basic business decision.

The browser, particularly **Internet Explorer (IE), is a very real source of vulnerabilities.**

## 4. Security Threats From Windows XP Come From More than Just Operating System Security Holes

The operating system is just one part of the overall software "load" that makes a PC useful. The entire software suite includes an Internet browser, and device drivers that enable the proper operation of a mouse, display and network connection. As Windows XP is becomes obsolete, **these elements of the software environment will also present potential security holes.**

The browser, particularly Internet Explorer (IE), is a very real source of vulnerabilities. Modern versions of IE (9.0 and later) are more secure and functional; however, they are incompatible with Windows XP.

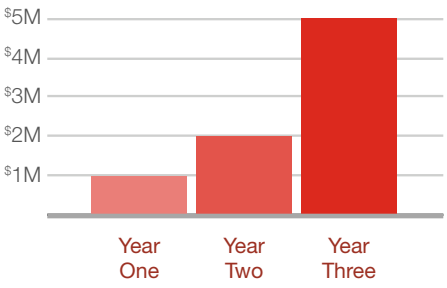
There is also one particularly troubling security problem for IE 8.0 that allows malware entry and gives the author full control of that system. Hackers use this vulnerability to install the "RAT Poison Ivy" malware, which gives them even more control of a single PC, and access to other systems.

The second, non-operating system software security threat comes from device drivers, the software that runs keyboards, displays, mice and other peripherals. Much like other aspects of Windows XP, updates to drivers are not going to come as quickly or as often as for newer versions of Windows. Additionally, many Windows XP systems contain peripherals that are much older and do not undergo the same scrutiny and testing as newer ones. This may result in undiscovered vulnerabilities and a lack of updates as the peripheral vendors consider these devices obsolete, much like Windows XP.

## 5. The Cost Of Supporting Windows XP After End of Life Is Substantial

Some organizations are just not willing to migrate from Windows XP and, as a result, have only one option for maintaining some level of support and the delivery of needed security patches: buying a Microsoft Custom Support Agreement (CSA) for Windows XP.

**Quotes for a Microsoft Customer Service Agreement** for 5,000 systems went from **$1 million in year one,** to **$2 million in year two,** to **$5 million in year three.**




As earlier stated, that this is a very costly approach. Gartner analyst Michael Silver has reported that the **quotes for the initial year of support are consistently in the $600,000 to $5 million range for the first year** (most quotes work out to approximately $200 per PC). It is also important to note that an unnamed IT manager in a recent *Computerworld* story reported that the quotes for a CSA for 5,000 Windows XP systems went from $1 million in year one to $2 million in year two, and to $5 million in year three! **For the cost of this CSA in years one and two, organizations could procure new devices and migrate their users.** Clearly, a CSA is not the most effective use of IT budget.

There are also substantial cost differences in the operation of Windows XP and Windows® 7 systems. The inefficiencies found in Windows XP for both IT and end users are pretty noticeable and compound the problem. Some of the key data points from a recent IDC study include the following:

- **Windows XP sees 27 percent more virus attacks** per month per PC than those using Windows 7
- The average number of **help desk hours needed per year per PC for Windows XP are 4.8,** compared to just 0.8 hours for a Windows 7 system
- **Average time to repair a malware attack is 3.7 hours** for Windows XP and 0.5 hours for Windows 7.

This amount of additional time and resources result in **substantially higher costs.** With the additional expense of the CSA after EOL, **organizations will face an uneconomical situation** that is more than enough to cost justify a migration away from existing Windows XP systems, wherever possible.

It's very clear that **migration away from Windows XP** is the **best course of action.**

## Conclusion

From a purely business perspective, **Windows XP's continued use after the April 8, 2014 EOL date creates a number of troubling problems for an enterprise.** These include:

- **The potential for corporate liability** based on breaches of personal information that can be traced to a Windows XP system.
- **Without a costly Custom Support Agreement, Windows XP systems will become vulnerable** as there won't be new patches to protect them otherwise.
- Management must be aware of the **substantial cost increases** that running Windows XP after its EOL will entail.

**This all adds up to a very lopsided equation with real risks and very little benefit.** Staying with Windows XP may save a few dollars in the short term and appease a few users. However, when weighed against the liabilities the costs, and the potential impact on the organization, **it's very clear that migration away from Windows XP is the best course of action.**

**Get more information about Lenovo's automated migration solution: In-Place Migration.**

## Sources


- "Begin Preparing For The End...Of Windows XP." *TechWeekEurope UK.*
- "Microsoft Admits Zero-day Bug in IE8, Pledges Patch." *Computerworld.*
- "Microsoft Gooses Windows XP's Custom Support Prices as Deadline Nears." *Computerworld.*
- "Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea (IDC White Paper)." *Microsoft Download Center.*
- "Operating System Market Share." *NetMarketShare.*
- "With Windows XP Security Updates Ending, Enterprises Must Plan Ahead." *TechTarget.*