Kingston Smith Consulting
Helping clients succeed

KSC Comment
Windows XP support ceased on 8th April 2014 – Frequently Asked Questions

10 April 2014; Mark Child, Partner at Kingston Smith Consulting LLP, answers frequently asked questions following the cessation of support by Microsoft for its Windows XP platform.

1 What is going on with Windows XP?

As of 8 April 2014, Microsoft has now ceased to support Windows XP, the operating system in use by a large number of enterprises. Windows XP was first introduced in 2001. Since that time, Microsoft has developed new operating systems (Vista, Windows 7) on which they now wish to focus their attention.

The company recently released a statement clarifying the matter:

> *Microsoft has provided support for Windows XP for the past 12 years. But now the time has come for us, along with our hardware and software partners, to invest our resources toward supporting more recent technologies so that we can continue to deliver great new experiences.*
>
> *As a result, after April 8, 2014, technical assistance for Windows XP will no longer be available, including automatic updates that help protect your PC. Microsoft will also stop providing Microsoft Security Essentials for download on Windows XP on this date. (If you already have Microsoft Security Essentials installed, you will continue to receive anti-malware signature updates for a limited time, but this does not mean that your PC will be secure because Microsoft will no longer be providing security updates to help protect your PC.)*
>
> *If you continue to use Windows XP after support ends, your computer will still work but it might become more vulnerable to security risks and viruses. Also, as more software and hardware manufacturers continue to optimize for more recent versions of Windows, you can expect to encounter greater numbers of apps and devices that do not work with Windows XP.*

2 What will this mean for organisations who use Windows XP?

From April 8, 2014, no new security patches for Windows XP will be produced. Microsoft will also no longer offer any technical support for Windows XP.

Windows XP systems won't stop functioning. You can continue to use them and even download old security patches, but no new ones will be produced.

As Microsoft has dropped support for XP, the industry will follow. New software isn't necessarily tested to work on Windows XP, and new hardware may not have drivers for Windows XP at all. The amount of software and hardware that doesn't support XP will grow.

3 Why should I care?

Microsoft will no longer provide any more security patches or support information for XP unless customers have a paid support plan.

"Security patches" are software providers' way of closing known gaps in the software which compromise the integrity of your IT infrastructure. With many vulnerable PCs now on the web, it is only a matter of time before unpatched vulnerabilities are identified and exploited. This will lead to a higher amount of botnet spam. It is also possible that these PCs will be harnessed for the distributed denial of service (DDoS) attacks.

The increased vulnerability of an "unpatched" Windows XP-based system means more chance of cyber-attacks, data breaches or competitors stealing company secrets[1].

4 How do I know if my organisation is affected?

Given that Windows XP was the most popular operating system in the world until August 2012[2], it's highly likely that Windows XP had some impact on your infrastructure.

Remember that, although sales of enterprise-level Windows XP licenses ceased on 30 June 2008, Microsoft continued to provide licenses for use on "ultra low-cost" devices such as netbooks until 22 October 2011.

5 My organisation moved to "the cloud" last year. Might we still be affected?

Although many cloud providers have up-to-date technology and interfaces, a number still rely on Windows XP at server level. Without asking specific questions as part of an IT audit, it's difficult to assure any organisation that they won't be affected by this change.

6 So if we upgrade our systems we will be ok?

If your organisation has a Windows XP deployment, you should already be working on migrating to a new version of Windows. If you're a home user, you should be looking at upgrading, too. Most longtime Windows XP users generally agree that Windows 7 is a worthy upgrade (Windows 8 is more controversial), and Microsoft will be supporting Windows 7 until 2020.

A system upgrade may solve the initial problem. However, the reality is that most organisations now have an interaction with a third party within their IT estate. These include:

- Payroll applications;
- E-commerce / payment applications;
- Specialist or industry-specific software packages;
- Banking applications;

[1] http://www.networkworld.com/community/blog/debunking-data-breach-myths
[2] http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=11&qpcustomb=0

- Client/customer portals;
- Financial or other databases.

Recent research quoted by the UK Information Commissioner's Office indicates that 77% of organisations "are running XP somewhere in their IT estate".[3] You should think carefully about the nature of the assurance you obtain from your third parties that they are taking steps to mitigate the risk. Will these providers consider an upgrade? Most organisations still employing Windows XP, which was launched in 2001, have already chosen not to undergo even one of three operating system upgrades since then.

7 What action should I take?

The first step should be to check with the people that provide your IT infrastructure and service whether they think your organisation will be affected. This is usually your internal IT team or your outsourced provider.

Are you happy with their answers? Given the potential risks from a Windows XP-based vulnerability are high, should you consider seeking independent assurance over what you have been told?

Finally, consider the number of third parties on which your organisation relies (see above at #6 for some examples). How will you go about obtaining confirmation from these third party providers?

This may present an opportunity for your organisation to reconsider your information security strategy. Many organisations now employ systems to mitigate the risk of malware or viruses. However, some recent examples of costly data breaches (leading to the loss of reputation) have come from:

- Insider leaks (BBC);
- Third party failure (Mastercard, Visa); and
- Failure by organisation to follow its own policies (NHS).

Is your information security strategy reflecting "best practice" in the market?

8 Are there any other Kingston Smith Consulting recommendations?

Kingston Smith Consulting is happy to answer any questions regarding any of the above answers or the issue in general.

We think this issue presents organisations with an opportunity to assess whether their current technology is a good fit for their organisational strategy (in addition to their information security and operational effectiveness).

We regularly see many clients with systems they don't need or fully understand. Many are not clear what they are paying for – and whether, in fact, they are getting value for money.

[3] http://www.computerweekly.com/news/2240217623/ICO-issues-data-protection-warning-on-Windows-XP?asrc=EM_ERU_27955624&utm_medium=EM&utm_source=ERU&utm_campaign=20140407_ERU%20Transmission%20for%2004/07/2014%20(UserUniverse:%20771181)_myka-reports@techtarget.com&src=5229875

If your service provider has not talked to you about this issue, it could be a sign that they have not yet finalised their transition plan. In any case, if you'd like independent assurance around your IT systems, information security or data protection, Kingston Smith Consulting would be happy to help.

Kingston Smith Consulting LLP

10 April 2014

About the author

Mark Child is a highly respected senior IT auditor and information security risk professional who has developed and directed international audit and risk functions in a range of sectors including financial services, retail and manufacturing. Mark is an acknowledged specialist in risk management, data privacy, internal audit and quality management and has managed the successful implementation of global projects and business initiatives.

Contact Us

Mark Child
Partner
Kingston Smith Consulting LLP
(0)207 566 3732
Mchild@kscllp.co.uk

or

Shourik Chatterjee
Senior Business Development Executive
Kingston Smith Consulting LLP
schatterjee@kscllp.co.uk
07880 433375