masonadvisory

WHITE PAPER

APOCALYPSE NOW?

Is it really the end of the world if you're still using Windows XP?

Given the apocalyptic hype around Microsoft ending support for Windows XP and Office 2003, organisations could be forgiven for feeling that the risk has been overplayed. If IT operations are continuing without security breaches, then some organisations may have let the issue slip off the priority list. In this white paper, Mason Advisory explains why heads of ICT shouldn't make this mistake, as well as providing some tips on things that can be done now to reduce the risk.

What's the threat from using out-of-support systems?

Since April 2014, there has been no support from Microsoft for Windows XP and Office 2003. As a result, technical assistance – including automatic security updates that help protect your PC – are no longer available. Organisations continuing to use Windows XP and/or Office 2003 are now more vulnerable to security risks and viruses. Furthermore, Microsoft announced that it will no longer support Internet Explorer (IE) 8, so any organisation using a Windows XP PC to surf the Web is exposing itself to additional threats.

Security experts anticipate new attacks identified by security researchers and hackers will now be launched in an attempt to exploit potential vulnerabilities within the legacy software. A common practice adopted to do this is to reverse engineer the security updates for later (supported) products. This process enables hackers to detect the specific section of code that contains the vulnerability addressed by the update. Once identified, this can be developed in an attempt to exploit legacy systems which share this code, but do not have the patched security updates.

Ultimately, for organisations still running Windows XP, time has run out. Microsoft estimates that the average migration to a new operating system takes between 18 and 36 months. Organisations are now at risk of compromising the safety of their data, which could subsequently cause reputational damage.

Figure 1: Infection rate (CCM) by operating system and service pack in 2Q13 [Source: Microsoft]1

> *Ultimately, for organisations still running Windows XP, time has run out.*

Can additional security help?

Firewalls and intrusion protection mechanisms such as sophisticated anti-virus software can only provide limited protection to vulnerable XP machines. As sophisticated as the security mitigations for Windows XP Service Pack 3 were when released, technology has moved on. Exploiting vulnerabilities now involve a variety of methods, including spear-phishing (legitimate-looking emails targeted at individuals inside organisations) and 'drive-by' attacks delivered using hacked Web pages or adverts on legitimate sites. The data in Figure 1, taken from a Microsoft Security Intelligence Report, shows that newer operating systems such as Windows 7 and 8 have a significantly lower malware infection rates than XP (even when Microsoft released security patch updates for the operating system). Therefore the security for XP machines is no longer adequate to protect against many of the attacks used today.

support one that runs Windows 7 or later.2 This difference has further been enhanced due to Microsoft stopping its support of XP in April 2014. Organisations now wishing for continual XP support require a special agreement with Microsoft. However, this bespoke support is not cheap. For just one year of prolonged support, the UK government is paying GBP5.5 million. With Microsoft saying prices will rise, keeping with XP might get very expensive. Furthermore, this is a stop-gap rather than a permanent solution. Large expenditure will still be required to update to a newer operating system further down the line.

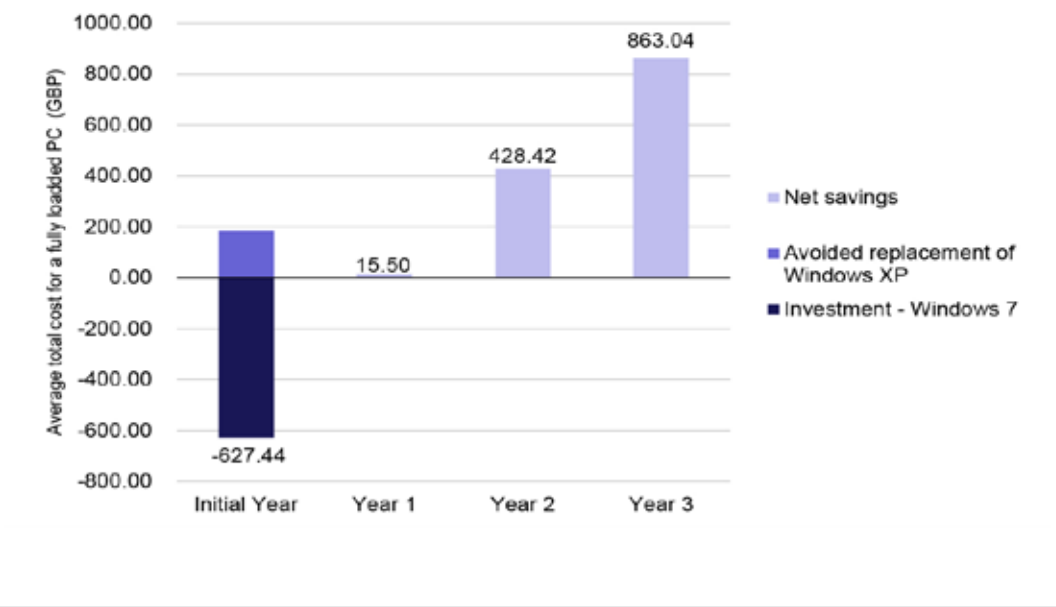
Isn't there an obvious answer?

The solution seems simple: migrate to later versions of the desktop operating systems within the Microsoft portfolio. However, in reality this is a complex task. Any such migration requires meticulous planning due to the numerous complexities associated with it. Nik Simpson, a research vice-president at market analysts Gartner, cited applications as being the key issue in any migration: "[U]pdating an operating system is relatively painless. Updating all the applications that run on top of it is something else entirely". This is largely to do with the changes introduced into Vista, XP's successor. That includes a security technology known as User Account Control (UAC), which limits what a user's account on a machine can do to that device. UAC subsequently broke older, sometimes business-critical, applications.

And there are other potential migration challenges…

Windows XP is not compatible with Internet Explorer (IE) after version 6. Therefore, it is common practice to upgrade the browser and operating system simultaneously. However, many intranet applications depend on IE6-specific features and behaviour, which can cause performance issues when migrated to later IE versions. IE8 and IE9 require developers to conform to more rigorous standards and rules. This means all intranet applications should be tested in advance in an attempt to identify any issues; furthermore, additional development may be required to ensure compatibility. Alternatively, the use of other browsers (such as Google Chrome or Mozilla Firefox) can be considered once Windows XP is no longer the underlying operating system.

Figure 2:
Return-on-investment analysis
[Source: IDC, 2012]



Microsoft Office applications released in Microsoft's 2010 and 2013 product suite have significantly different user interfaces. New icons, new menus and other changes mean there is simply no way of getting around the usability issues that changing an operating system will have. Significant effort should be taken by organisations in an attempt to minimise the loss of productivity to end users. More significantly, however, from Office 2010 onwards, the file type associated with products in the Office suite changes, for example Word and Excel files become .docx and .xlsx respectively. Although conversion tools are available to allow older versions of Office to open these file types, there are still numerous compatibility issues.

In addition to those alluded to above, organisations will face additional migration challenges, such as hardware incompatibility and data loss.

The solution seems simple: migrate to later versions of the desktop operating systems within the Microsoft portfolio. However, in reality this is a complex task.

Other than avoiding the risks, are there any other benefits to migrating?

As well as the risks of continuing with Windows XP, Figure 2, based on IDC estimates, shows there is an upside. It provides a three-year return-on-investment analysis of the payback associated with a move from Windows XP to Windows 7.

There are also less tangible knock-on effects. According to Paul Miles, a Project Manager in the John Lewis Partnership IT department who oversaw the "enormous exercise" of upgrading 26 000 devices to Windows 7, those included:

- happier staff, who enjoy the more up-to-date software and faster machines
- the chance to jettison old, redundant applications
- a much better idea of what is sitting on the computers of employees
- updated and more robust recovery and back-up plans.3

...continued overleaf

So what can organisations do today?

As already noted, a company-wide migration takes years to plan and implement. But there are several steps that an organisation can take immediately while preparing for the long-term eventuality of a footprint without Windows XP.

Where possible, eliminate all Web browsing and external email on XP desktops – two predominant vectors where security issues are likely to come through.

Engage rapidly with Microsoft to determine the availability, scope and costs of customised support for XP.

Virtualise. Use remotely hosted thin-client environments to provide browser and mail client support to XP users or use sand-boxed virtual environments to provide Web and email capabilities.

Ultimately, these are short-term solutions to mitigate risk. Moving to a newer operating system will still be crucial.

Notes: '32' = 32-bit edition; '64' = 64-bit edition.
SP = Service Pack. RTM = release to manufacturing. Operating systems with at least 0.1% of total MSRT executions in 2Q13 shown. [Microsoft Security Intelligence Report, Volume 15, January–June 2013] IDC, Mitigating Risk, Gillen, Selig, Perry http://www.bbc.co.uk/news/technology-28790582

About Mason Advisory

Mason Advisory is trusted by the public and private sectors to provide independent advice and support. As an IT consultancy within the Datatec Group, we understand that technology can transform the way organisations operate and perform – but only when it's designed and deployed effectively. You can be confident that we'll help you get those critical decisions right, with over 20 years' experience of supporting organisations from strategy development through to implementation and assurance.

Contact us

If you would like to discuss the issues raised in this article, please email us at contact@masonadvisory.com or call +44 (0)161 772 3305

www.masonadvisory.com