Strategies for Windows XP in 2014

On April 8, 2014, Microsoft will cease updating Windows XP. This means no more support, no more bug fixes and, more prominently, no more security "patches" that plug security holes.

See the Microsoft information on this at:

http://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

This will make computers running Windows XP increasingly vulnerable to targeted security attacks. After all, Windows XP will remain with a considerable fraction of the operating system landscape and, thus, a worthy target as it becomes more vulnerable to the rapidly-evolving threats.

You might ask: ***"Isn't Windows XP just going to stay the same as it is now? Perhaps no better but just the same? What will make Windows XP more vulnerable?"***

- Yes. As of April 8, Windows XP will stay the same after that date but it won't be supported.
- In that sense, it will certainly be no better and it ***will*** worsen due to external forces.

The security landscape works like this:

Experts continue to seek out vulnerabilities. These experts can be "black hats" or they can be "white hats" – depending on their motives. Either way, the newly-found vulnerabilities are widely known throughout the computer community. So, it's the newest, most recent, threats that one needs to be the most concerned about. Most of the parasites we remove are new ones. The old ones have pretty much been covered by fixes and in the security software suites.

Supported operating systems, like Windows XP is today, are continually being modified to resolve those newly-found vulnerabilities. When support stops, new vulnerabilities will continue to be found and exploited while the fixes will no longer be made.

One might ask: ***"Won't my antivirus and security software continue to evolve and protect my computer?"*** The answer would be "maybe" and "don't count on it". It depends on which vulnerability mechanism is being exploited. Is it something that can be protected against? Is an operating system fix (that won't be coming) really what's needed? Further, how much effort will commercial companies put toward protecting an out-of-support operating system? They likely won't or won't for very long. That's just good business practice: to focus on where they get the most leverage for their investment. We predict that some security software companies will stop supporting Windows XP perhaps as early as Microsoft stops supporting Windows XP.

The question for users and owners of Windows XP is ***"what shall we do about this"?*** If you can buy a new computer or tablet or smart phone and get everything you want done then no worries. "Getting everything you want done" may be a bit harder than you think – so please read on. If buying a new computer (or a building full of them) is too costly or if you might be stymied by some of the nuances, then you will want to consider the options like:

1) Stick with it.
2) Isolate the Windows XP computers
    a. Disconnect the internet
    b. Use virtual environments
3) Migrate / jump to computers with a newer operating system like Windows 7 or 8.1

Sticking with it, even with shored-up security is a matter of accepting a risk. At the same time, it has the least up-front cost which could be as low as zero. The benefit of zero or low up-front cost essentially pushes cost risk forward in time. "How risky this is?" becomes the question.

A risk assessment could be a great step forward in supporting a decision to "stick with it". (The assumption here is that the computer has internet access one way or another). If the computer has no internet, network or outside data access then the risk assessment is pretty much over. Just make sure this remains the case!
A risk assessment should include estimating the degree of "risky connectivity" as well as the risk of loss due to any compromises. Historical performance and loss can be a central guide.

One needs to be concerned with a number of things regarding vulnerabilities:
- Need my data be protected and secure?
- Is there an investment in time and money in the computer configuration itself?
- Is having the computer up and running in a short period of time essential?
- Can my critical application work on a newer operating system?

Need my data be protected and secure?

Maybe all you need is to have your data backed up. Maybe the world doesn't end if it gets leaked somehow. And, maybe it's sensitive and you can't afford to reveal it in any way.

Is there an investment in time and money in the computer configuration itself?

Some office computers only need to have the operating system intact and have an office suite installed and email available. The investment in creating these configurations is small. So the configuration may not need to be saved because the cost of saving it may outweigh the cost of reproducing it.

Other computers may have very comprehensive and integrated applications installed. Some computers may have even been configured by engineering teams and can't be readily reproduced (e.g. in an industrial controls environment). It's these cases where the investment is high and the computer configuration should be ready for being reconstituted. In fact, this may be advisable no matter what the operating system!

Is having the computer up and running in a short period of time essential?

If the answer to this question is "yes" then while there may not be a large investment in the configuration, there is a large cost in not having the system up and running. So the concern is the same as the case with large investment.

Can my critical application work on a newer operating system?

Below, the notion of migrating to a newer operating system is discussed. One of the pitfalls is that some of your existing printers on Windows XP computers will not work

with a newer operating system. That old printer you use for printing labels? If you have to continue to use that old printer then maybe it's best to set up a Windows XP "printing station" just for the purpose of continuing to print those labels. That's an example of "sticking with it".

Coastal Computers & Networks can help you implement "stick with it" strategies and can help you set up system images for quick recovery.

Migrate the operating system generally suggests keeping the computers involved or gradually replacing them. "Jumping" just means going directly to a new operating system once and for all. (The likelihood of keeping the old computers is low and isn't recommended to be pursued unless the computers are quite new and very capable). Either way, this approach carries the risk, even the certainty, that some things will no longer work. Some printers will have to be retired along with the computers. Other peripheral devices will have to be retired as well (such as scales and other instruments and specialty printers for labels or postage). Some number of application programs won't run on the new system. This could be of no import or could be a show-stopper. The older the software, the greater the risk it won't work. Of course, one workaround for application programs could be to upgrade the application to a version that's compatible with the new operating system. Yet there are some great old programs around that have no new versions available. And, the more specialized the program and the more investment in its implementation and deployment, the greater the concern.

One strategy for migration that can work well in small offices or home offices is to set up a new computer alongside an older Windows XP computer, put them on the local network and share at least the XP computer files. A program like Kavoom KM can be used to share the keyboard and mouse while using a separate monitor for each computer. Then, the work is really about moving data into the new computer and installing the needed applications while retaining all the current capabilities. This takes some focused effort because the objective is to retire the old computer in a reasonably short time.

Isolating the XP computers is a way to remove them from external threats. The biggest threat is removed by disconnecting the internet connection. Even if a machine is compromised by secondary means (see below) then the path for sending critical data to the outside world is removed.

Removing the internet connection can be a simple as pulling out the network cable. Of course, disconnecting the network means no more web browsing, email ,etc. on this computer. It also means no more file sharing even over the local network. Access to files and outgoing transfer of files means using CD/DVD/USB media. Even if such an apparent unwieldy approach is used, there are particular security measures that should be taken. In general, this means you won't want to do this with applications that rely on much data transfer.

More sophisticated approaches can be used to keep XP (and other) computers on a local network while isolating them from the internet and from computers that have internet access. This means that industrial networks (for example) can continue to operate with Windows XP and share local data while providing protection against threats. Doing this requires particular networking expertise.

Virtual environments come in a variety of programs and products that allow Windows XP or Windows XP application programs to be run within the context of newer, supported, operating systems such as Windows 7 or 8. This means that the underlying computers will be capable of being connected to the internet and local network as always. And, it means that older programs written for Windows XP can often run on a newer system. But, security precautions in doing this remain as outlined here.