Microsoft XP support ending - April 2014

iVoice Systems may be at Risk!

Microsoft will stop offering security and performance updates for its elderly operating system, XP, after in April 2014. Soon to follow will be third party application vendors and their software updates for XP (i.e. Java, Adobe, Google Chrome…). However, this may still not raise the red flag and convince customers to upgrade their equipment. The excuse, "it works and has been working for years so I don't need to upgrade", is a common attitude.

We assume that customers maintain these systems and run the Windows updates as part of their normal business processes and keep their O/S's up to date with the Microsoft security patches as they are released. These patches primarily are provided as vulnerabilities are identified/detected. They are commonly released every second Tuesday of the month. Because operating systems are not built from the ground up, such vulnerabilities affect multiple operating systems from XP to Windows 7 and 8. For example, from July 2012 through July 2013, Windows XP received 45 patches, 30 of which were relevant to Windows 7 and 8. After April 2014, when support for XP ends, patches will still be provided when such vulnerabilities are detected but will not be released for XP making it more susceptible to attacks. Hackers will reverse engineer the patches and apply their new knowledge and efforts towards systems running XP.

A scary fact - Windows XP is still almost ubiquitous in organizations which have to adhere to strict privacy and security standards, including the banking, finance, security and healthcare industry. Windows XP was seen as the go-to operating system for ATMs, with almost 75% of ATM machines in the US running Microsoft's relic of an operating system. How this will be addressed is still unknown at this time.

PCI Compliance

You probably know that any site that accepts credit cards has to have SSL Encryption. You also might know that they are routinely subjected to security testing, to ensure the website itself is free of security vulnerabilities. Well, this is part of a larger package called PCI-DSS, which sets up a bunch of prescriptive rules that companies have to adhere to. Using an operating system that no longer receives security updates is a big no-no.

Should a non-compliant company find themselves the victim of a security breach, they can be guaranteed a hefty fine by the Payment Card Industry.

Upgrade the O/S and all will be rosy

The obvious solution is to upgrade or replace the operating system but what does this mean? In most cases you cannot just upgrade the operating system and continue on with business as usual. Upgrading the operating system, in boxes that have old hardware, will likely lead to compatibility issues. Drivers may not be available for older hardware running with the newer operating systems. In addition, do you really want to "try your luck" with hardware that is nearly as old as the XP operating system? Is that good business practice?

The best solution is to upgrade the iMessaging System iVoice controller to a new and supported operating system, Windows 7 - fully supported by Microsoft for years to come. New hardware with

current support and the most current drivers available will ensure that you are protected and compliant. New features such as encryption, Spanish language support, and a new Text-to-Speech application are available as well. Consider it an investment in your companies' security and peace of mind. We know that iVoice is a product where in many cases, you "set it and forget it" but it's time to actually think about it. With some systems 7 years or older, can you really sit back and relax without taking action? Who will they run to when the system is identified as non-compliant or becomes unavailable?