

Security is an ever growing concern for clinics of all sizes. Data security used to consist of locking the office doors at night before leaving with a box full of charts that need completing. With the introduction of wireless notebooks, off-site billing companies, lab companies, and branch offices, clinics are now faced with an ever-changing array of security related responsibilities, many of which seem unnecessary or overwhelming to a physician who simply wants to concentrate on quality patient care, not technological security needs. So this begs the question: How important is it to ensure that patient data is secure? According to a study by the Ponemon Institute in 2007,^[1] an organization specializing in privacy and information management research, data breaches cost companies an average of \$197 per patient record. So the simple answer is, very important.

Operating System Security

In this series, I am going to address various security concerns that clinics will face if they do not make data security a priority, as well as offer suggestions that will assist physicians in making security decisions. In part one of this series I will cover the daunting task of upgrading your operating system to fit your needs. Hopefully, your office has moved to a professional operating system for both your workstations and your servers. The ability to protect a document at the file level is a key part in maintaining security in your environment. If you are in a Windows environment, this is obtained by using an operating system that supports New Technology's File System (NTFS) by Microsoft. NTFS was introduced with Windows NT 3.1 in 1993 and has been a staple of professional operating systems ever since. Home based operating systems, such as Windows 95, 98 and Millennium do not support NTFS. They use the File Allocation Table (FAT) file system, which allows any user that is logged on to the computer access to all files and folders on that workstation. A server that utilized the FAT file system could be accessed remotely to easily view all files and folders and even worse, deleted. Another limitation of FAT32 is a file size limit of only 4 GB, which may not be large enough to house an EHR database or a personal email folder. Once the file reaches the file size limit, the file may become corrupt. The term "Security" previously had been used simply to describe one's ability in terms of file access. Either a user could access the data or not. Today, clinics need to control the exchange of data not only within the office, but also between satellite offices and hospitals.

Over the years, operating systems have tried to provide some of the security for us, but only if you know which operating system to buy. It is hard enough to choose a workstation in an electronics superstore that encompasses more than just computers, but the fact of the matter is that it is a pretty solid bet that none of the machines on display will

come loaded with a professional operating system. A professional operating system is designed to network and secure businesses of all sizes and it will come at an additional cost. When Windows XP Professional was released, by default, no blank passwords were allowed. User accounts with blank passwords could only log on locally. The account could not be used for remote access to the machine or access to network shares. Suddenly, clicking "OK" at the log-on screen, if applicable, would no longer suffice for accessing network shares. The sudden inconvenience of entering a password was now being enforced. By adding a few more clicks and keystrokes to everyone's daily processes, order was restored and everyone was able to access their shares via entering a password. The world's technical support lines' false sense of tranquility was short lived; however, until the release of Windows XP Professional Service Pack Two. Windows XP Professional SP2 was intended to protect us from mischievous Internet traffic by introducing a built-in firewall that was turned on by default. The result of this automatic update was a firewall at the workstation level that monitored and more often blocked all traffic in or out of the machine. This sounds good from a security standpoint, but unfortunately for many, the traffic that was blocked included connections to EMR databases, lab results and bills. A "System Down" situation after an operating system upgrade is not going to encourage an office to perform future upgrades anytime soon.

"THE ABILITY TO PROTECT A DOCUMENT AT THE FILE LEVEL IS A KEY PART IN MAINTAINING SECURITY IN YOUR ENVIRONMENT."

Windows Vista

The latest operating system in the Microsoft family is Vista and along with it comes some of the most thought out security yet. From an IT standpoint, the most noticeable difference in Windows Vista is the User Account Control (UAC). All users run in what is called standard user mode. The UAC now allows users to perform most standard functions without the need for administrative privileges. I remember when all users on the domain had to be at least a Power User on Windows 2000 Professional to be able to run the spell checker in Outlook. This is no longer the case, because the UAC even changed the definition of the "Administrator" account. The "Administrator" account no longer has full control over the entire system. Administrators are able to perform most functions, but any potentially dangerous changes require authorization from the user. A standard user now has the ability to perform more functions, such as installing print drivers

and applications, but an administrator will have to authorize potentially dangerous changes. In simple terms, users are now able to perform daily work functions without involving an administrator as often, yet malware or the user cannot overwrite the kernel or the registry without authorization from an administrator. Microsoft even applied this theory to Internet Explorer 7 (IE7), which is loaded with Windows Vista. In addition to a 256-bit cipher strength, IE7 offers Protected Mode, which has even fewer privileges than the standard user mode in Vista. IE7 is restricted by the UAC, so it is only allowed to write to the Temporary Internet Files folder. This is a major enhancement in the area of securely browsing the Internet. Malware can no longer install programs or change the home page along with other configurations in the operating system.

Now that some of the security features that have been added to operating systems over the years have been explained, the plot is about to thicken a little bit more. One key detail about Vista that has not been mentioned is that Windows Vista is available in 6 versions, including Windows Vista Starter, which is designed for users in developing technology markets and is not available in the United States. It is fairly self explanatory that if the title contains the word "Home", then it is not designed for a business, but the reason is not immediately clear. This would include Windows Vista Home Basic and Vista Home Premium. Windows Vista Home products cannot be added to a domain, so document management and securely sharing information is an immediate concern. Unfortunately, these two operating systems are most likely to be preloaded on any machine that you buy online or off the shelf. These operating systems are centered around entertainment media, such as burning cds and viewing dvds. They are not the right choice for a professional environment. It will come as no surprise that Windows Vista Business can be added to a domain. The only other differences between Windows Vista Home Premium and Business is that Business does not include the entertainment packages such as Windows Media Center, Windows DVD, Movie Maker HD, and Parental Controls. For a small to mid-size practice, Windows Vista Business will most likely be the most cost-effective solution.

Windows Vista Enterprise helps in the area of centralized administration and virtualization by allowing the use of diskless, virtual PCs that can boot remotely, so no data is stored locally on the machine. This feature is very popular in a hospital environment that contains several mobile PCs that could be stolen or damaged. Vista Enterprise also allows up to four virtual operating systems to run on one machine.

This comes in handy for multiple databases running on the same machine while keeping the information separate. Vista Enterprise has also added the BitLocker Drive Encryption security feature for hard drive encryption, which is disabled by default. The main drawback of Vista Enterprise is that a small to mid-size clinic may not see the need to implement all of the security capabilities that are available in Vista Enterprise. This may result in Vista Enterprise not being a cost-effective solution, because it is only sold with a volume license. Windows Vista Ultimate is an all-inclusive version that is actually geared more towards the consumer rather than an office environment. There is no added functionality in the area of security, other than the BitLocker module that is also included with Vista Enterprise.



Summary

Hopefully this article has pointed out some of things to consider when buying new hardware or upgrading an operating system as well as protecting data on the workstations and servers. Additional cost should be considered in the budget to achieve the level of security that you desire. As always, all new operating systems should be tested before implementing them across the whole company to make sure that all of the clinics' applications will run successfully. If an application will not run on Vista, the application can be tested in compatibility mode, but running an application in compatibility mode will reduce the level of security, because the UAC will be disabled for the application that is technically running under a different operating system. In future articles, I am going to cover protecting data for mobile users, data that is sent over wireless networks and information that is sent over the Internet to branch offices or vendors.

Jamie Osborn, MCSE, MCDST

Director of Support, MediNotes Corporation

Jamie Osborn is the Director of Support with MediNotes Corporation. He manages a team of 22 Technical Support Specialists at the company's headquarters in West Des Moines, Iowa. Serving more than 23,000 users, in over 4,700 clinics nationwide, Mr. Osborn and his team effectively answer over 90% of incoming technical calls in one minute or less. Mr. Osborn holds a Bachelor's Degree in Computer Science from the University of Northern Iowa and has been with MediNotes for over five years.

References

1. Ponemon Institute (Nov. 2007). "2007 Annual Study: U.S. Cost of a Data Breach", p.2.