THREE KEYS TO LIMITING YOUR EXPOSURE

It's always a good time to review some basic security practices that can help limit the exposure of your company to data loss or theft. Implementing some or all of the following steps can greatly enhance your company's security and limit your exposure to unplanned costs and liabilities.

Staying Secure – While most people are aware of the need for strong passwords (passwords containing a mix of numbers, letters, and symbols), there are additional steps you can take to protect the information on your computer.

One of the simplest methods is to enable a BIOS password on your computer. The BIOS is the system that runs in the background of your computer, and allows Windows to talk to the hardware of your computer. The BIOS loads onto your computer first, before Windows, and by requiring a password you effectively stop Windows from loading until the password is supplied.

Another method to protect the data on your computer is to encrypt any files you wish to keep private with a personal key. You then share a public key with other users that you wish to have access to the file, allowing them to unlock the file and view its contents. This insures that if someone does gain unwanted access to your data, they cannot use it without your decryption key and can be used to protect sensitive financial data and intellectual property.

Control Access – While many companies allow access to the internet with little restriction, the risk of virus infection from malicious websites has been on a dramatic rise over the last few years, with virus creators becoming all the more sophisticated with their method of attack. These viruses are often costly to remove, if they can be removed at all and can result in permanent data loss. While modern anti-virus suites do a fair job of preventing and catching infection, the best layer of security is to prevent general access to the internet, and allow only the sites necessary for the business.

An additional threat to unlimited access is that many media publishers are pursuing legal action against those that download illegal copies of music, movies, and software. This could put your organization at risk if users are downloading from work.

Stay Managed – The common tendency of most people is to not think about their computer environment until there is a problem with it. However, many common computer issues can be prevent or minimized well in advance of an actual problem. A service like Trinity's ActivSurveillance™ runs a small agent on every workstation and server in your organization, which reports back any errors in the hardware or alerts from the operating system, anti-virus, or back-ups.

About the Author:
Joshua Slick is a Network Engineer with Trinity Worldwide Technologies providing technology information to small and medium size businesses via our e-newsletters, blogs, and websites.