Impact of PC Administrator Access on Unlicensed Software Exposure

By Brian Von Hatten

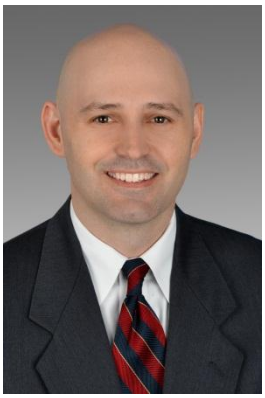
Operating system level security in the workplace has always been a double-edged sword. Everyone generally recognizes its importance, but internal customers need more, and IT departments are faced with increasing help desk requests while managing with a continuously shrinking number of resources. In an effort to "resolve" many help desk requests before they come, IT administrators will often leave user accounts either with admin access during deployment or perhaps during some sort of resolution phase of an open trouble ticket.

What this means is that if a user is a "restricted" user, then that user will likely not be able to install software that would require a license. When user accounts are given admin access (or less) on their computer, they are able to install software. The question is, does this expose companies to greater risk of having unlicensed software in their environment?

One problem that may arise is the installation of programs that are free for individual use, but not for commercial use. Another possibility is that users want to run productivity tools which they historically utilized at a previous employer, but which the current employer is not licensed for. In this case, the user brings a "copy" in to work one day and installs a fresh and unlicensed copy of the software. This concept is particularly bothersome given that IT administrators (other than locking down the user account) may not know about or condone such activity. This brings to light the need for IT departments to audit their own software installations.

A quick search regarding this topic revealed a state university's administrator access request form available on the public Internet.[1] It is worth noting that the form includes the following affirmation from the requesting party: "I will not use my administrator access to install any pirated or unlicensed software on university computers." It should be pointed out that regardless of how unlicensed software finds its way into your workplace, the company's potential liability remains largely the same. Most piracy actions are brought pursuant to the U.S. Copyright Act, and because Copyright Infringement is a strict liability crime, the intent that one use unlicensed is not required, and lack of knowledge is generally not a defense.

We may never know what percentage of unlicensed software in the workplace is caused by unsuspecting users, but one thing is for sure–it can be extremely costly. Contact Scott & Scott, LLP to discuss ways to ensure compliance *before* the audit letter comes.



About the author Brian Von Hatten:

Brian represents many large and mid-market organizations on matters related to transactions, software licensing, and disputes. Brian's focus includes substantial attention to complex information technology issues for companies of all sizes.

Get in touch: bvonhatten@scottandscottllp.com | 800.596.6176

[1] http://www.sulross.edu/sites/default/files//sites/default/files/users/docs/admin/administrator_access_policy.pdf