Open source software, OSS, is software that is shared at all levels. For instance, the source code that makes it perform or function the way it does is available for all to see. Also, you can choose to use it as is or make changes to it. You can inspect the original version of the code or any and all modifications of it. And of course all of this is possible because everyone would share their respective documentation. Open source software doesn't necessarily mean free. Anyone could charge for the use of OSS. The real question is will anyone pay once they can see "what's behind the curtain."

Here are a few reasons why open source software is significant to security. First, having open source software will let all see the code which will hold the programmer(s ) accountable for their code. This will hopefully eliminate sloppy coding which could lead to security exposures. Second, with open source, the exposure window could theoretically be shortened. With many users finding bugs and writing patches for these bugs the opportunity presents itself to have a shorter exposure window. Obviously, a shorter exposure window translates to fewer systems being at risk. Third, the user can make an informed decision on what software to purchase. If you are looking for software to perform specific security measures and have the opportunity to evaluate an open source package, then you have options. You could evaluate it yourself or have it scrutinized by experts to see if it meets your requirements. Knowledge is power, and the more knowledge you have about a potential software package the more power you will have over security.

You can't have security without controlling confidentiality, integrity, and availability. Open source software can significantly improve security through such

measures. Confidentiality is only allowing authorized users access to “X” (the system, data, or information). With OSS you can verify and/or modify the code to make certain that only authorized users have access. Integrity is maintaining a pristine version of “X”, and any modifications to “X” are only made by authorized users. By using OSS you can again verify that all elements, internal or external, that have the potential to corrupt the integrity of “X” are eliminated. Accessibility is having constant access to “X” especially during an emergency. It is well documented that viruses, and the like, can make it hard to access “X”. OSS will lessen the exposure window that could hinder accessibility to “X”.