Open Source Rewards and Risks: A Due Diligence Must

Advisor: Open Source –082709

There is obvious benefit and inherent risk in buying or investing in companies who develop software applications or systems for resale using Open Source. Open source code review is a must-have on the due diligence check list. Knowing the pedigree of the software used in development is an absolute requirement – for its positive business rationale as well as assessing liability.

Four Risk Factors

Along with the many benefits of open source code there are a number of risks according to the Software Licensing Committee of the American Bar Association.

- **Potential liability for Infringement:** Perhaps the most obvious risk is potential liability for intellectual property infringement. The typical open source project contains contributions from many people. This method of development can be worrisome from an intellectual property standpoint because it creates multiple opportunities for contributors to introduce infringing code. The risks of this development process are largely borne by the licensees. Contributors may not vouch for the cleanliness of the code they contribute to the project; in fact, the opposite may be true -- the standard open source license is designed to be very protective of the contributor.
- **Shift of Risk to Developer/Licensee:** The typical open source license form does not include any intellectual property representations, warranties or indemnities in favor of the licensee; it contains a broad disclaimer of all warranties that benefits the licensor/contributors. Many of the most prominent open source projects appear to be owned by thinly-capitalized non-profit entities that do not have the financial wherewithal to answer for a massive intellectual property infringement suit. The shifting of all risk for intellectual property infringement to the licensee is atypical for the commercial software world. Most for-profit software companies would require some level of contractual assurances from a licensor of software technology that such technology does not infringe intellectual property rights.
- **Doubtful Ownership of Derivative Works:** When investing in companies developing with open source software one needs to consider the problems associated with creating derivative works. Some open source license forms, such as the General Public License (GPL), require licensees to provide free copies of their derivative works in source code form for others to use, modify and redistribute This licensing term makes it very difficult for companies in the commercial software business to use

such open source software as a foundation for a business because their "value added" programs might some day be viewed as "derivative works" and need to be made available to the world in source code form for free.

- **Multiple Contributors:** Some open source projects have multiple contributors and modules that have been created under various licensing forms. According to the terms of most open source licenses, the licensee must give each of these contributors full copyright attribution and reproduce the entire text of the license agreements for the open source code included in the product. These notices and licenses can clutter up documentation files and confuse end user customers.

Four Mitigating Factors

Copyright infringement is a crime and in order to protect themselves and their customers from potential legal, ownership, and business interruption issues, enterprises developing applications or investors buying/funding companies using open-source software need to:

- **Assess the code base**: It is important to note that when an enterprise or investor decides to assess the code base, the first investigation is the most important. The entity who conducts that investigation is also critical as is the process which needs to be managed to get the best and most accurate information. Consideration must be given to preserve attorney-client privilege when undertaking such an assessment so as to allow the information flow to be controlled and to limit the number of people involved in the investigation.
- **Evaluate the processes that are in place**: Once a decision is made to assess the code, projects should be prioritized and the entire code base should not be assessed at once. One project should be reviewed at a time and that review should be completed before the next review is started.
- **Undertake remediation:** The most difficult issue companies face, after such a code review, is tracking code that has been distributed to third parties and answering the question of what their obligations are to notify third parties. Before doing so they need to fully understand the way the third party uses and redistributes the code as well as the third party's obligation to install an update.
- **Roll out a compliance program:** Establish a due diligence policy and implement automated end-auditable business controls. Companies need to evaluate existing procedures, both the formal and informal ones, as well as identify opportunities to capitalize on the benefits of using open source.

A Valuable Solution

Semaphore has long provided open source code review to its industry staple Technology Diligence practice in order to assist its clients with code inventory and review. The Semaphore solution includes appropriate use of Black Duck Software in

the cases where an automated and memorialized review is appropriate. This can be employed on a going forward diligence review, post integration plan execution or forensic evaluation when required Conducting such review by an organization with a full understanding of software use, investor/acquirer interests, legal attenuation, market risks and remediation capacity is helpful to those operating executives tasked with making an investment or acquisition work as well as to those General Counsels who are burdened with the obligation of heeding the risks and mitigating the liabilities replete within the open source world today.