Open-Source Risk

Legal, security, and operational dangers in your software

By Jonathan Hobbs, founder and director of Hobbs & Associates

Open-source software is everywhere and in everything. Today, 90 percent of smartphones are based on Android, 75 percent of cloud platforms run Linux, and 70 percent of websites are built on WordPress, Joomla, or Drupal. What has contributed to the extraordinary growth of open-source software? First, in most cases, it's free (though licensing obligations do apply).

Open-source software is developed and curated by online communities of professionals, and in most cases the code is stable. Communities such as GitHub have nearly 40 million open-source projects available for download. The use of open-source is growing at a non-linear rate. In 2007, there were 200,000 open-source projects. In 2017, that number is expected to exceed 2.5 million.

Sounds ideal, but there are risks; and these fall into three main categories: legal, security, and operational.

Legal open-source software is free—in the sense that, in most cases, there are no licensing fees—but all open-source software is subject to various licensing compliance obligations. Open-source software is also subject to infringement of intellectual property (IP) rights and, in most cases, affords no IP rights.

There are many different types of open-source software licenses, the most common of which is the general public license, version 2 (GPLv2). Under GPLv2, any modifications to open-source code must be made available to the development community. This could mean that incorporating a piece of open-source software into your code base would require you to make your entire source code available for public reuse, making any vulnerabilities in your code open to exploitation by nefarious hackers.

There are also intellectual property issues to consider. Tens of thousands of software-related patents have been granted in the United States dating back more than 50 years. A patent guarantees the patentee a monopoly on, and protection of, their invention for a limited time.

Given the long history of software patents in the United States, it is almost certain that many open-source projects are infringing on some patents. A company's right to protect software-related innovations are blocked by the license obligations in most open-source software agreements. Many companies learn that their innovative software product cannot be patented after the fact. Having invested hundreds of thousands of dollars in developing unique software, these companies are now at risk of competitors copying their products.

SECURITY

Serious security vulnerabilities in open source-software appear in the news almost every day. According to Matthew Jacobs, vice president of general counsel at security firm Black Duck Software, Inc., serious security vulnerabilities in open-source components turned up in more than 65 percent of the code bases that Black Duck audited last year. Malware such as Ghost and vulnerabilities such as Heartbleed and Shellshock are just the tip of the iceberg.

Risks related to the unmonitored use of open-source software to business operations are often revealed during a merger and acquisition (M&A). As software has become a larger part of the valuation during an M&A, the acquirer wants to know exactly what operational risks are involved. As a result, audits for open-source components have become a requirement during an M&A in the United States.

The entire business model of many organizations is software-related. Software-as-a-service business models rely entirely on software for operations. The risks of unmonitored open-source vulnerabilities directly impact the bottom line of these businesses, and could mean the difference between success and failure.

There is no doubt that the use of open-source software will continue to rise. This increase requires a vigilant and proactive approach to code-base management. A clear understanding of the legal, security, and organizational risks with regard to your business is the first step in this process. ■

Risks related to the unmonitored use of open-source software . . . are often revealed during a merger and acquisition.