

Liability and Control Risks with Open Source Software

David Bahn
College of Management
Metropolitan State University
Minneapolis, MN.
david.bahn@metrostate.edu

Dan Dressel
College of Management
Metropolitan State University
Minneapolis, MN.
dresseda@go.metrostate.edu

ABSTRACT: An exploratory investigation was conducted on the liability and control risks posed to U.S. organizations by the adoption of OSS. Three primary risks associated with the use of OSS were identified: upstream intellectual property concerns, viral software issues, and non-infringement warranties or intellectual property (IP) indemnity issues. In the context of a field investigation of these risks, several potential scenarios of OSS risk to organizations were identified, with two of them appearing as primary. The first primary scenario is the potential loss of control over revenue generating proprietary software when OSS source code and proprietary software source code are mixed together in one primary software works. The second primary risk scenario is the potential loss of control over software products or services offered within an organization due to legal disputes about intellectual property (IP). Other secondary risk scenarios are discussed as well. Some emerging trends in this area are also reviewed.

Index Terms - Open Source, Risk, Controls

I. INTRODUCTION

Organizations are increasingly making use of open source software (OSS) to supplement internal software development efforts or to displace proprietary software offerings. Software is largely a service industry operating under the persistent but unfounded delusion that it is a manufacturing industry [15]. OSS empowers users by allowing them to control the software rather than allowing proprietary software vendors to control the software [21]. This is a powerful shift of control that involves a certain amount of business risk. OSS introduction within an organization needs to be done in a methodical fashion to ensure that business risks are minimized.

An exploratory study was conducted of the risks engendered by the introduction of OSS into organizations. Field investigation and literature review were utilized to

identify and categorize these potentials risks, as well as identify several potentially resulting scenarios of risk to organizations.

II. OPEN SOURCE SOFTWARE

Before discussing the business risks and liability issues of using open source software, it's important to understand the fundamental concepts behind Open Source Software (OSS). The frequently used terms "free" and "open source" are often combined to create the Free and Open Source Software (FOSS) label. The key difference between the meaning of "free" and "open source" in the open source community is the type of license used for the software. The Free Software Foundation's (FSF) advocacy of free software relies nearly exclusively on the GNU General Public licensing (GPL) (as well as parallel licensing models that are classified as GPL compatible) in order to enforce that (a) software remains "free" of any software royalty charges and (b) that a degree of source code sharing when software is distributed. The GPL license contains a copyleft clause, which is used to counter copyrights that typically take away freedom. A copyleft, which is a play on the term "copyright," grants reuse and reproduction rights to everyone. The copyleft clause specifies that when new versions of the original works, also called derivative works, are distributed then others are granted the rights to use, modify, and redistribute the source code. A copyleft makes the source code and the freedoms legally inseparable.

By contrast, the Open Source Initiative's advocacy of OSS not only approves the GPL and GPL compatible licenses but also endorses several other "open source" licenses that are not approved by the Free Software Foundation. Some of these additional licenses (for example the Berkeley Software Distribution (BSD) license) are considered more "friendly" to commercial business requirements because they do not contain stipulations mandating the sharing of derivative works [8].

However, both free and open source software are in direct opposition to proprietary software licenses that restrict

access to source code. OSS differs from proprietary software in three ways. First, users have access to the human readable software source code, whereas proprietary software is almost always distributed in object code format only. Second, the users can freely copy, distribute, and modify the software, whereas proprietary software almost always prohibits that type of use. Third, open source software is licensed free of charge, whereas proprietary software is almost always licensed for a fee [4].

III. RISKS OF OPEN SOURCE SOFTWARE

A) *Open Source Risks*

As previously stated, OSS risk factors are manifest in three main areas. Upstream intellectual property concerns are manifest as code is transferred between parties and difficulties grow in separating OSS from proprietary software. There is resulting increased risk that code believed to be free is actually proprietary and requires a license fee. The use of OSS causes infringements on an unknown piece of proprietary code that leaked into the OSS. The resulting lawsuits could burden an organization with unexpected expenses and potentially lead to injunctions that impact business operations [6].

Viral software issues are a second risk that surfaces as the use of OSS leads to the mandatory release of internal proprietary software code. The use of both proprietary and OSS within increases the risk that an organization's key business applications may be believed to be proprietary but may contain some OSS [1]. The unintended inclusion of the OSS could then cause the organization to risk losing control over some exclusive competitive advantage as it becomes required to release internal software source code [20].

Non-infringement warranties or IP indemnities are a third source of risk. These are issues that surface when using OSS that lacks standard warranties and intellectual property indemnity protection. For example, a lawsuit claiming an IP rights violation leaves an OSS user financially responsible to defend and settle a legal claim. While this is changing in connection with some OSS products, most OSS is used "as is" and susceptible to intellectual property attack [20].

B) *Perception of Risk Factors*

The business community's response to these risks for the most part has ranged from limited concerns over the use of OSS to extreme concerns that include complete restrictions on OSS use. Organizations that rely on proprietary software code to drive business value are obviously concerned about the potential to lose control over the revenue generating proprietary source code. Organizations that are primarily users (rather than developers) of business software have a perception that OSS use is high risk, but in reality this is most likely a very low risk for them [1,8].

The business law community sees OSS as having the potential for major legal issues if not controlled properly

within organizations. The potential legal issues include patent infringement lawsuits and third party intellectual property claims that could lead to problems with core business operations. Law community experts view OSS users as having potential legal issues because OSS lacks warranties and IP indemnities [2,14,20]. With minimal case law in the realm of OSS, many legal decisions remain unresolved.

IV. SCENARIOS OF RISK TO ORGANIZATIONS

A) *Mixing Proprietary and Open Source Software*

The upstream intellectual property (IP) risk involves the contaminating of OSS with proprietary software that requires a fee to use. The "for fee" proprietary source code is included in the OSS without knowing an IP violation occurred. At a later time, the IP violation is recognized and the OSS is no longer considered OSS but rather requires a fee-based license [20]. This could lead to an organization having to pay for software that was once thought to be free as well as to liability claims for IP violations such as copyright, patent, or trade secret violations.

Conversely, the viral software risk of contaminating proprietary software with OSS could cause the proprietary software to become OSS. The GPL type licenses contain copyleft and derivative works clauses that subject the source code to OSS rules [20]. It is not uncommon for companies to publish company policies and procedures that ban the use of GPL licensed software when there is any chance that OSS could be integrated with the company's proprietary software development efforts [16]. Software development firms must keep proprietary software separate from GNU GPL software, so the proprietary software is not exposed to GPL licensing requirements [1,8,11,17,19]. Theoretically, an OSS license can change from one model of license into another but only if proper permissions are granted by all copyright holders [19]. OSS sometimes assigns the copyright permissions to a central authority like the FSF. In the case of Linux the copyright ownership has not been assigned to a central authority, so it would be very difficult to change the underlying license used for Linux. A Linux licensing change, for example from GPL to a BSD type license, would require all the individual copyrights holders to agree to the license change [12]. While theoretically possible, it is highly impractical.

As different OSS licensing models are deployed within the same software project, the licenses can become incompatible with each other, thus causing an entanglement of difficult legal concerns and issues [18]. For example, does one license take precedence over another license or does the license incompatibly invalidate both licenses? This is the kind of legal question that can end up being very costly to answer, especially in a situation of litigation.

In addition, the very nature of the GPL license model could cause an organization's entire software portfolio to

become open source if that portfolio is not assembled correctly [1,16]. The GPL's derivative works clause raises concerns for any new software development effort that involves a mixture of OSS and proprietary software in the development environment.

Admittedly, one significant exception to the concerns about the viral nature of the GPL has been the widespread acceptance of Linux. As system software, Linux can be deployed in a way that facilitates its remaining distinct from proprietary application software components running on top of it. This has enhanced the adoption of Linux despite its use of the GPL license. As companies review OSS to determine the impact of allowing the software to be used, any GPL licensed software needs to be clearly separable from proprietary works to avoid risks of exposing the proprietary software [1,8,11,12,17,19].

B) Intellectual Property and Liability issues

Other scenarios of risk for organizations stem from the lack of warranties or intellectual property (IP) indemnification for OSS [20]. A legal injunction involving a patent, copyright, trade secret, or other IP issue could bring an organization's entire business to a halt. The most common concerns relate to patent and trade secret issues because they tend to entail a much broader scope. OSS is normally delivered as is with no warranty or indemnification as noted in the licensing agreement. A copyright issue, unless it is a very broad violation that includes several software components, is generally easier to resolve and fix than a patent issue [19]. Moreover, a patent issue will almost always be broad in scope such that if a violation occurs it could result in a court injunction that would bring a business' application platform to a halt. In as much as an injunction is a legal decision based on information provided to a judge, the issue is subject to legal interpretation [16]. Legal decisions are very difficult to predict when it comes to intellectual property issues surrounding patents and trade secrets. Copyrights violations are usually easier to prove and resolve but they can also incur legal expenses and possible injunctions depending on the scope of the violation.

As patent lawsuits continue to increase in the legal system, more organizations are applying for patents in an attempt to protect themselves from costly legal challenges at a later time and to protect original ideas from being stolen [16]. In the OSS community the source code is very visible and copyright ownership is tracked with the source code. Source code visibility allows many people to review the actual source code. The concern over time is that OSS contains proprietary copyrighted source code that would not be identified until a legal action is taken against the OSS. In general, copyright issues are less of a concern than other IP issues such as patent or trade secret issues, although copyright issues still warrant attention and can lead to legal issues [19]. As a protection

mechanism, organizations and individuals can register copyrights and obtain patents in order to clearly document the ownership of source code.

Closely related to the aforementioned scenarios is the issue of liability for an organization's product or services that are improperly delivered due to problems with the reliability OSS. Disclaimers in many of the open source license agreements have provisions that state a licensee has no recourse if the open source application proves to be unstable, malfunctions, provide erroneous output, or otherwise fails to perform [13]. A lawsuit could limit the ability of a company to sell a product or service during the legal proceeding [16,18]. Some of the proprietary software vendors provide protection, indemnification, for legal issues that directly involve the software they sell. Another factor underlying the acceptance of Linux is that vendors have stepped up to offer some indemnification against pending and potential lawsuits against Linux IP [16]. Understanding the scope of indemnification coverage is important because any software developed using an indemnified piece of vendor software will most likely not be protected using the vendor indemnification coverage [19]. Indemnification usually does not provide legal protection for products or services that are built using the vendor software tools unless the legal issue is directly related to a component solely owned by the software vendor.

Most software license contracts are specially designed to avoid accident liability risk for the vendor that sells the software, so proprietary and OSS software generally provide no additional accident liability protection. This is indeed one of the key reasons that proprietary software is sold using a license rather than sold as a product [12]. There is some debate about whether software is a product or a service. There is growing evidence, however, that courts will consider software a product [3,10]. Unless specially stated in a software license agreement, a software license does not provide any legal protection from product or service accident liability issues associated with faulty or defective software.

V. OTHER RISK CONSIDERATIONS FOR OPEN SOURCE

Several secondary issues of risk with OSS were also identified in this investigation. Some of these are independent of the three primary risk factors and some are not.

A) Employee Use of Open Source Software

An organization is responsible for setting rules of conduct for its employees. Organizations need stated policies and procedures against misuse of all types of IP including but not limited to patents, copyrights, and trade secrets. Organization will be responsible for any illegal use of software source code by employees and will need to correct such situations. If the company can prove that an employee was malicious in intent they should have an opportunity to correct the issue [1]. The resolution of legal issues associated

with the misuse of software source code will most likely be complicated and will be dependent on the exact nature of the violation [16].

B) *Potential for Viruses in Open Source Software*

OSS is normally delivered as is with no warrantee or indemnification as noted in the licensing agreement. There is really no difference between OSS and proprietary software when it comes to protection against hackers. Software license agreements are used to protect the owner of the software from lawsuits related to software issues involving such things as viruses and bugs [7,8,12]. OSS hosting sites used to download OSS provide no financial protection against business issues caused by viruses in the downloaded software [8].

C) *Merger and Acquisitions Responsibilities*

Open source considerations may affect the representations, warranties, indemnities, value and structure of a merger or acquisition transaction [7]. Almost all merger and acquisition (M&A) transactions that take place in today's business environment include language related to OSS. The language often contains statements that assure OSS IP is fully disclosed during the M&A transaction as well as statements that assure OSS license compliance rules have been followed [1]. Both OSS and proprietary software license agreements must be fully understood with all violations and exceptions resolved during the M&A analysis.

During an M&A, the purchasing company must perform a due diligence inspection of all software code to avoid the risk of legal issues after the M&A is complete. This is particularly important if a company is being acquired for its software IP assets. If the assets are thought to be proprietary in nature and later found to contain OSS, the assets could be found to violate OSS licensing agreements and thus become property of the OSS community during a potentially expensive legal battle [1].

VI. EMERGING TRENDS

Emerging standards and guidelines are starting to form that stress the importance of tracking OSS utilization [1,5,8]. Depending on the size of the organization, the level of automation used for OSS tracking will vary. The first emergent standards and guidelines are that organizations must develop well documented policies and procedures about OSS use within the organization [5].

The emergence of automation, especially for larger companies, appears to be gaining attention in the marketplace. Two vendor products that sniff out OSS software use within an organization are Black Duck's ProtexIP software and Palamida's IP Amplifier software [5,9]. These two companies are the emerging market leaders in the detection and tracking of OSS. The ability to detect and track OSS with automated software will likely continue to gain acceptance over manual detection processes.

REFERENCES

- [1] A. Aitken, Olliance Group, Managing Partner. Phone Interview on April 12, 2005.
- [2] H. Amir Khalid, "Open source still faces open legal questions," Retrieved from http://www.qbit.gr/contents/news.php?go=on&n_id=209&screen=0&res_t, October 12, 2005.
- [3] J. Armour & W. Humphrey, "Software Product Liability," Carnegie Mellon University: Software Engineering Institute (CMU/SEI-93-TR-13), 1993
- [4] P. Brown, "Beyond SCO v. IBM: Other Legal Issues in the Open Source Community," in *Open Source Software: Risk, Benefits & Practical Realities in the Corporate Environment*, S. Davidson, & S. Levi, Eds. New York: Practising Law Institute, 2004. p. 114.
- [5] S. Davidson & S. Levi, *Open Source Software: Risk, Benefits & Practical Realities in the Corporate Environment*. New York: Practising Law Institute, 2004.
- [6] L. DiDio, "Indemnification Becomes Open Source's Nightmare and Microsoft's Blessing," The Yankee Group, November 2004.
- [7] R. Fresquez, "Open Source Software Considerations: For Managing Open Source Software Risks In M&A Corporate Transactions," The Open Source Technology Alliance, 2005
- [8] C. Garry, MetaGroup, Research Analyst. Phone Interview on February 1, 2005.
- [9] L. Greenemeier, "Sniff Out Open-Source Code," *InformationWeek*, p. 59, May 9th, 2005.
- [10] S. Hurd, A. McMullin, P. Shears, & F. Zollers, "No more soft landings for software: liability for defects in an industry that has come of age," *Santa Clara Computer & High Technology Law Journal*, v21 i4 p745(38), May 2005.
- [11] G. Kloke, Open Technology Systems, President and Founder. Phone Interview on March 14, 2005.
- [12] J. Lerner, & J. Tirole, "The Scope of Open Source Licensing," *Journal of Law, Economics and Organization*, 21(1), pp. 20-56, Spring 2005).
- [13] M. Overly. *The Open Source Handbook*. Maryland: Pike and Fisher, 2003.
- [14] D. Ravicher, "Mitigating Linux Patent Risk," Open Source Risk Management position paper, Retrieved from www.osriskmanagement.com/pdf_articles/linuxpatentpaper.pdf August 2, 2004.
- [15] E. Raymond, *The Cathedral & The Bazaar*. Sebastopol, CA.: O'Reilly & Associates, Inc., 1999
- [16] M. Stignani, Intellectual Property Attorney. Interview on May 12, 2005.
- [17] M. Webbink, M, "Open Source Software – Bridging the Chasm." In *22nd Annual Institute on Computer Law*, P. Brown, K. Williams & J. Yates, Eds. New York: Practising Law Institute, 2002, pp. 669-679.
- [18] G. Weinstein, Faegre & Benson, Partner & Intellectual Property Attorney. Presentation at Metropolitan State University, Minneapolis, Minnesota, April 27, 2005.
- [19] J. White, CodeWeavers, CEO and Founder. Phone Interview on April 21, 2005.
- [20] J. Yates & P. Arne, "Balancing the Scales – Managing Risks in IT Projects." In *24th Annual Institute on Computer Law*, P. Brown, & K. Williams, Eds. New York: Practising Law Institute, 2004, pp. 121-122.
- [21] B. Young, "Foreword by Bob Young" In *The Cathedral & The Bazaar*, Raymond, E. Author. Sebastopol, CA.: O'Reilly & Associates, Inc.