

A Framework for Managing Risk When Using Free & Open Source Software (FOSS)

Phil Robb

Director, Open Source Program Office, Hewlett-Packard

General Manager, FOSSBazaar.org

© 2008 Phil Robb, Hewlett-Packard,
Creative Commons Attribution License 2.5



THE OPEN FORUM
FOR HIGHER EDUCATION EXECUTIVES

Introducing Phil Robb

- Software engineer since 1982
 - Mostly Unix internals and networking stack
- Turned full time manager in 1999
- Started working in the FOSS community in 2001 @ HP
- Member of HP's Open Source Review Board since 2001
- Currently...
 - Director of HP's Open Source Program Office
 - Coordinate HP's involvement in FOSS Technical Conferences
 - Lead HP's efforts in Governance Tools and Governance Consulting
 - General Manager of FOSSBazaar.org

FOSS is Unavoidable

- Established Markets have been pillaged
 - Compilers Toolchains & Development Environments
 - Enterprise Operating Systems
 - Embedded Operating Systems
 - Web Servers
 - Established Strongholds have been weakened
 - Oracle, Weblogic, IBM all now offer “Free” or “Community” versions.
 - New Markets Never Began
 - Web Service protocols / Java Tools & Libraries
 - MS compatible File and Print Services
 - Very difficult for a commercial co to invest what’s needed to
 - engineer a samba competitor then try to charge for it’s use
 - Blogging & Wiki Software
- * Most (soon to be all) Proprietary Software will contain open source software

FOSS' Adoption: Businesses and Governments

Early Adopters:

- spend time and effort to make a new technology work
- Put up with imperfections in the early product versions

Early Majority:

- Need the product to be easily consumed
- It must either fit into the existing structure, or..
- The differences must be well understood



Why is FOSS Different Than Commercial Software?

To use commercial software in your development process you must go through...



Procurement!

How is the FOSS you use chosen?

- Fitness for a particular purpose?
- License terms?
- Size of the community
- Age and activity of the community?
- Direction & health of the community?
- Any clouds of IP litigation looming?

How is the FOSS you use acquired?

Did the code come from the single authentic source repository (sourceforge, Berlios, etc)?

Did the bits arrive intact?

- Was the MD5 checksum matched?

Was the project compiled from source?

- If not, what assurances exist that the binary has no malware?

How and where is the FOSS used?

- Is the FOSS used only internally or is it distributed?
 - Do outside contractors work on the code?
- Is the FOSS co-mingled with proprietary code?
 - Is that allowed via the FOSS license?
- Are all the FOSS licenses compatible with one another?
- How mission-critical is the FOSS-based application(s)?
- How many groups use each FOSS component?
- Are other groups using similar but different components or different versions of the same component? Is it absolutely necessary?

How is the FOSS you use supported?

Self-support?

- How good are the ties to the community?

Commercial Support (SpringSource, RedHat, Novell, MySQL, Symas, etc)

- How to deal with different stack component vendors?

Commercial Support (Integration vendors: HP, OpenLogic, SourceLabs, Spike Source, etc)

- Is the company stable enough to persist?

How is the FOSS you use tracked?

- Who tracks vulnerabilities and critical defects posted against the FOSS component(s)?
- How do those component rolls get into the company's development cycle?
- Who tracks the health and roadmap of the project(s)?
- How often, and to whom do they report the status?

Intellectual Property Risk

Copyright Infringement – License Infringement

- FOSS Licenses represent the culture & intent of the communities that use it
 - Understanding the intent & philosophy of the copyright holder is key
- Reciprocal Licenses (Source code must be distributed with the binaries)
- GPLv3
 - Patent Implications
 - Anti-Tivoization provision
- Affero GPLv3
 - SW functionality delivered via network (web) must also provide source code

Intellectual Property Risk

Patent Infringement

- Patent Trolls
 - Can no longer attack prey one at a time
 - Groklaw
 - Starfire v Jboss (Red Hat)
- Market exclusion
 - Most technology companies rely on FOSS
 - Open Invention Network (OIN) exists to defend Linux from Patent litigation
 - Technology company's customers are FOSS users
 - Once disclosed, the FOSS community will rewrite to avoid patent
 - entanglements

Finally, it is proving very difficult to litigate against the FOSS commons

Two New Communities Focused on FOSS Governance

FOSSology.org

Tools

- Discovery
- License detection
- Framework

FOSSBazaar.org

Best Practices

- Assessment
- Policy, process and workflow
- Breadth of use cases

More to come...