What Developers, Cars & Banks Have in Common: Best Practices for Open Source Governance

Shoken Kim
Black Duck Software

Linux Con Japan
Compliance Mini-Track

June 7, 2012
Overview

- Trends
- Strategic use of open source
- Management challenges
- Governance best practices
- Compliance in supply chain
Open Source Software – Market Trends

“Software is Eating the World.”

Marc Andreessen

“Open Source is ubiquitous...having a policy against open source [use] is impractical and places you at a competitive disadvantage.”

Mark Driver, Gartner
The Virtuous Cycle – Innovation and FOSS

600,000+ FOSS projects
100+ billion lines of code
10 million person-years of work

For more statistics about open source trends, projects, & developers, go to:
www.blackducksoftware.com/oss/projects
www.ohloh.net
“Open Source is a ‘silver bullet’ that allows simultaneous improvement along the dimensions of the “iron triangle” of cost, schedule, features.”

Jeffrey Hammond, Forrester (Aug. 2010)
Average represents the portion of FOSS in the overall codebases of 500 large enterprises surveyed by Gartner (January 2011)
Strategic use of FOSS

“Over 80% of the software in our handsets is open source”

Carl-Eric Mols, Head of OSS, Sony Ericsson Mobile Communications
“Super OSS Communities”

Healthcare
OSEHRA

Aerospace
Polarsys

Automotive
GENIVI

Finance
openMAMA

Mobile
Android

Copyright © 2011 Black Duck Software, Inc. All Rights Reserved.
Automobile Supply Chain – SW Everywhere

100+ m lines of code in a premium-class car
(IEEE, Feb. 2009)

70+% is in IVI “head unit”, at R&D of US$1-10/line!
(GENIVI, 2010)
IVI HeadUnit – No Longer “Just a Car Radio” Increasingly OSS-based & Costly
Financial FOSS Readily Available for Functions that were once only provided by ISVs.

"J.P. Morgan’s CDS Analytical Engine now available as open source code"
Strategic use of FOSS: Large Commercial UK Bank Trading Application

Delivered a new trading app but only wrote 35% of the code!

- Open Source Code (277MB), 65%
- Unique Code (120MB), 28%
- Code Duplicated with Other Projects (18MB), 4%
- 3rd Party Commercial Code (10MB), 3%
Management Challenges

“50% of companies will face challenges due to lack of FOSS policy and management”

OSS Analysis (Nov. 2011)
Open Source Adoption – Stages
Automated Governance and Compliance

Application development cycle:
- Plan
- Code
- Build
- Test
- Release

Build

Manual processes:
- Vulnerabilities
- Cryptographic
- License
- Maturity...

Manual processes:
- Legal
- Development
- Support

Manual vs. Automated Governance and Compliance

Legal

Compliance

Support

Cost

Risk

ID code

ID provenance
Automated Governance and Compliance

Application development cycle:
- Plan
- Code
- Build
- Test
- Release

Open source governance lifecycle:
- Acquire
- Approve
- Catalog
- Audit
- Monitor

Black Duck Knowledge Base

Description
Version
Vulnerabilities
Cryptography
License
Maturity...
Requirements for FOSS Governance

Strategy
- Articulate the business objectives for use of FOSS

Policy & Process
- FOSS policy & management process

Technology
- Automate governance and compliance
- Design-in and automate policies
Best Practices for Managing Open Source

- Adopt and enforce an open source policy
- Identify and track all external code that is used
- Automate validation at the point of acquisition and development
- Automate monitoring and tracking
- Use automation tools to audit and produce complete software Bills of Material and management reports
Compliance in a Supply Chain is a Challenge

One Product =

Many Suppliers
Many OSS Packages
Many OSS Licenses
SPDX™ and Software Bill of Materials

A standard format for communicating a software Bill of Materials across the supply chain.

Benefits:
• Reduced effort
• Reuse analysis
• Improve compliance
Case Study: OSS Benefit Realization

- Trip planning
- Airport process
- Boarding
- Flight
- Arrival

- Extent of use
- Licences
- Derived works
- Contributor

- Type of OSS
- Distribution
- Origin
- Support

Copyright © 2011 Black Duck Software, Inc. All Rights Reserved.
The use of Open Source Software without a governance program represents a major business risk.
Case Study: OSS Benefit Realization

Establish key stakeholder group

Strategy, policy, process

License review

Discovery & remediation

Approval

Communication & training

Open Source Governance (OSG) program
Case Study: OSS Benefit Realization

Risks
- Brand impact
- Security vulnerability
- Customer service
- IPR impact
- Legal infringement
Case Study: OSS Benefit Realization

Risks:
- Brand impact
- Security vulnerability
- Customer service
- IPR impact
- Legal infringement

Mitigation:
- Open Source Governance (OSG) and Automation
Case Study: OSS Benefit Realization

Combine the best of propriety and open source software components to bring ground-breaking and innovative solutions like Horizon* to market better, faster and more cost-effectively than ever before.”

Patrick Holden, Senior Program Manager, Software Development
About Black Duck Software
FOSS Enablement for Multi-Source Development

“Enable organizations and developers to build better software faster by automating and managing their selection, use and governance of FOSS”

Founded in 2002. Backed by industry leaders

Recognized as a market leader & innovator

Cool Vendor 2010
Application Development

“Nifty 150”
Cloud Computing

Innovation Award 2011
Thought Leadership

Events, White Papers, Webinars

- **Application Development & Management**
  - Develop Less, Produce More: How New Tools, Processes & Free Code are Redefining Software Development
  - Open Source as a Strategic Business Enabler: A Case Study with SAP

- **Legal**
  - Understanding the Top 10 Open Source Licenses
  - An Introduction to Open Source

- **M&A and Technical Due Diligence**
  - Open Source Due Diligence in M&A and Financing
  - Technical Due Diligence for M&A: A Perspective from Corporate Development at SAP

- **Open Source Think Tank**
  - Semi-Annual Event (Paris and California)
  - Brings together C-level executives and the world’s top FOSS thought leaders
FOSS Citizenship

- Actively supporting Linux Foundation
- Co-chairing SPDX: standard for exchanging code content/license info
- Ohloh.net & Koders.com; Foundations & Forges collaboration
- Participants in several FOSS development projects
- Olliance thought-leadership: Open Source ThinkTank, CEO dinners

Best practices:
- FOSS readiness checklist, sample FOSS policies
- Webinar series: legal, application development
- Best practices customer case studies
Your Guide to Open Source

Ohloh is a new kind of software directory, combining community-driven content with a unique source code crawler that monitors up-to-date development activity.

Search Projects
Ohloh's objective reports and community feedback help you find the software you need.

Search People
Open source is open collaboration. Find people who use and create open source.

Commit Volume
Discover how much each developer is contributing to a project, e.g.

Ohcount

Counting 16,103,209,601 lines of code

Most Popular Projects
- Mozilla Firefox: 10319 users
- Subversion: 7937 users

Most Active Projects
- Gertoo Linux: 16046 commits
- OpenX: 6186 commits

Most Active Contributors
- Michal Čihář: 1925 commits
- PatrickLauer: 812 commits