How to keep developers happy and lawyers calm
Presenter

Rod Cope
CTO
Rogue Wave Software
rod.cope@roguewave.com
Agenda

1. Introduction
2. Common OSS myths
3. Risks and challenges of OSS
4. Developers and lawyers
5. Q&A
**DILBERT**

**CAN YOU APPROVE THE PURCHASE OF THIS SOFTWARE?**

**YOU NEED TO RUN THE SOFTWARE LICENSE PAST LEGAL FIRST.**

**YOU NEED TO FILL OUT A LEGAL SERVICES REQUEST FORM. I'LL EMAIL IT TO YOU.**

**MAKE SURE YOU SPECIFY WHETHER THE SOFTWARE IS OPEN SOURCE OR NOT.**

**HOW WOULD I KNOW IF IT MEETS YOUR DEFINITION OF OPEN SOURCE?**

**IT DEPENDS HOW THE LICENSE IS WRITTEN. YOU'LL NEED TO ASK LEGAL TO REVIEW IT.**

**NEVER MIND. I'LL JUST FORGE YOUR SIGNATURE ON THE FORM.**

**MAYBE THIS IS WHY I'VE NEVER SEEN A SOFTWARE LICENSE.**

**BY SCOTT ADAMS**
Introduction
Legal disclaimer

• Rogue Wave Software, Inc. is not engaged in the rendering of legal advice. This training class material provides legal information, which should not be confused with legal advice

• I am not an attorney
Common OSS myths
MYTH: It’s free so I don’t have any license obligations

FACT: Copyright law protects authors, many have taken licensees to court or taken other legal action.
Common OSS myth

**MYTH:**
It’s in the public domain, so I can use it anyway I want

**FACT:**
Only some OSS is public domain
All other is protected by license or copyright
MYTH:  It’s free, so unlike commercial software, I don’t need to track it

FACT:  Many vulnerabilities in commercial software are due to OSS
If there’s a license violation how do you remediate?
Common OSS myth

**MYTH:**
I don’t need support

**FACT:**
Yes, you do.
What do you do if your system goes down at 2 a.m.?
Risks and challenges of OSS
## Legal risks and challenges

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Copyright</strong></td>
<td>Without proper permission you may lose right to use</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>Potential legal action for non-compliance</td>
</tr>
<tr>
<td><strong>Patents</strong></td>
<td>Use of OSS may force loss of patent rights</td>
</tr>
<tr>
<td><strong>Indemnification</strong></td>
<td>No protection from damages</td>
</tr>
</tbody>
</table>
Security

OSS can introduce security flaws and vulnerabilities into your software

Quality

OSS can potentially affect the quality of your application
Support & contribution risks and challenges

Support
Who do you call when you have a problem?

Community
Is contribution to OSS allowed?
# Managing risks

<table>
<thead>
<tr>
<th>Knowledge</th>
<th>Learn and understand the risks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Become a stakeholder in your organization’s risk management</td>
</tr>
<tr>
<td>Action</td>
<td>Take steps to manage OSS</td>
</tr>
<tr>
<td></td>
<td>Be active in compliance process</td>
</tr>
<tr>
<td></td>
<td>Monitor and track OSS you use</td>
</tr>
<tr>
<td>Understand and manage cost of OSS use</td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td>Support</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
</tr>
</tbody>
</table>
Developers and lawyers
Developers have a job to do

- Don’t add process that will unduly slow them down
- Don’t ask them to do additional jobs that take them away from their real job
- Don’t create rules or processes that take away ability to use OSS
Developers will use OSS regardless of policies (intentionally and un-intentionally)

- Blog articles, stack overflow
- Commercial products that contain OSS
- Code reuse (other in-house code that contains OSS)
- Indirect acquisition (code developed by contractors, outsourcers)

Moral: You can’t really stop use of OSS unless you have your developers write every line of code they use.
How open source enters your codebase?

Open source community

- Supply chain code
- Internally developed code
- Reused code
- Third-party components
- Legacy code
- Outsourced code

Production code
Developers aren’t malicious, unless they are

Your developers are stakeholders in your success, they’re NOT going to sabotage their own efforts.

As stakeholders, they have no interest in violating licenses, or creating a situation where your company gets sued for copyright infringement.

If provided the right information developers will use OSS in a way that reduces risks.
They don't expect developers to understand law any more than developers would expect lawyers to understand how to write code.

They do expect developers to understand basic concepts of law like how licenses work, what is a copyright, and how things like patents can be affected by OSS.

OSS may reshape the way developers and lawyers work together.
How lawyers and developers work together

Ignorance is a powerful force

• If developers don’t know there’s an issue they don’t know to ask a lawyer for help

• Creating boundaries can help developers know when it’s okay to use OSS and when to ask for legal assistance in determining risk

• An open dialog on OSS issues between legal and development builds on itself to reduce risk and workload associated with OSS over time
So how do you keep developers happy?

When it comes to using OSS:

<table>
<thead>
<tr>
<th>OSS awareness education</th>
<th>Simple processes and guidelines that don’t slow development</th>
<th>Tools or services to manage OSS</th>
</tr>
</thead>
</table>
| • By arming developers with basic knowledge of risks of OSS you empower them to identify, manage, and mitigate risks | • Developers don’t want to guess what to do with regards to OSS  
• Guess = ignore | • Don’t make it harder than it has to be |
How do you keep lawyers calm?

<table>
<thead>
<tr>
<th>OSS audits</th>
<th>Process for reporting OSS usage</th>
<th>OSS usage guidelines</th>
</tr>
</thead>
</table>
| • Outsource an initial audit of products (developers don’t need to do the work, and outsourcers who specialize in OSS audits will provide comprehensive assessment of current risks) | • Make development teams (now armed with their new knowledge of OSS) report all OSS usage going forward as they download
• Delineate based on license types and usage                                | • At one extreme that can mean a company-wide OSS policy defining every aspect of OSS
• At the other, it can be a simple set of guidelines designed to mitigate risk and plans to deal with issues as they arise |
Developing a compliance process

- Compliance actions
- Audit
- Review licenses
- Usage model
- Compliance checklist

Open Compliance Source
What developers need to know about OSS

How OSS is defined by your organization

The difference between a commercial and an OSS license

Guidelines and policies

Copyright, patents, indemnification, disclaimers of warranty, and liability

OSS license compliance

Managing and monitoring OSS
Training sources

• Linux foundation OSS compliance material and training
  – https://training.linuxfoundation.org/free-linux-training/linux-training-videos#compliance
  – https://training.linuxfoundation.org/linux-courses/open-source-compliance-courses/compliance-basics-for-developers

• OpenChain project
  – https://www.openchainproject.org/curriculum

• Rogue Wave Software Open Source Awareness training for developers
  • www.roguewave.com
Conclusion

Know your risk
- Legal, security, support

Proactively manage your OSS and compliance
- Track, monitor, comply

Remember: Benefits of OSS far outweigh risks
- Time to market, innovation, NO LICENSE FEE, readily accessible, robust community

© 2017 Rogue Wave Software, Inc. All Rights Reserved. 29
Q&A