



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

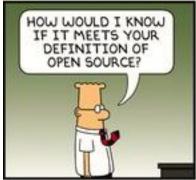
BY SCOTT ADAMS



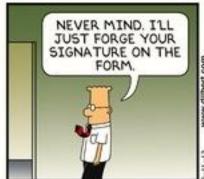


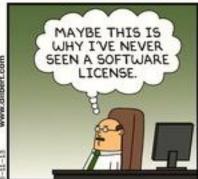












Introduction

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





MYTH:

It's free so I don't have any license obligations

FACT:

Copyright law protect authors, many have taken licensees to court or taken other legal action



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?



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

Copyright	Without proper permission you may lose right to use
Compliance	Potential legal action for non-compliance
Patents	Use of OSS may force loss of patent rights
Indemnification	No protection from damages



Technical & security risks and challenges

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

Knowledge	Learn and understand the risks
	Become a stakeholder in your organization's risk management
Action	Take steps to manage OSS
	Be active in compliance process
	Monitor and track OSS you use
Understand and manage cost of OSS use	Training
	Support
	Maintenance



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

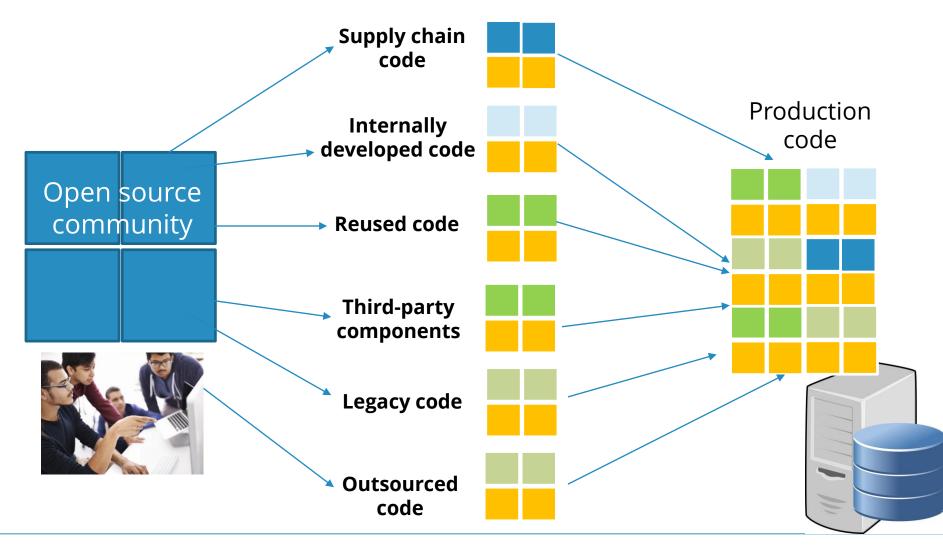
Code reuse (other in-house code that contains OSS)

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?





Developers aren't malicious, unless they are

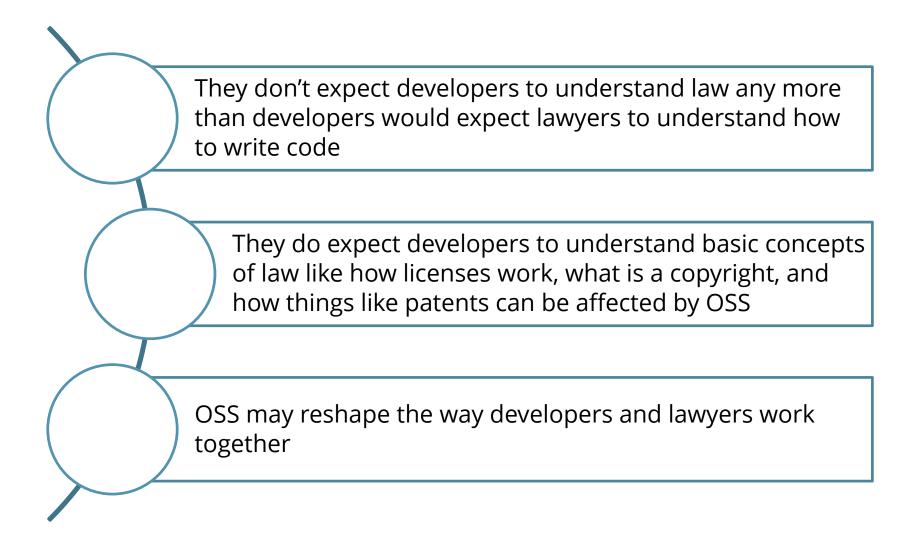
Your developers are stakeholders in your success, they're NOT going to sabotage their own efforts

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



Lawyers have a job to do





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:

OSS awareness education

 By arming developers with basic knowledge of risks of OSS you empower them to identify, manage, and mitigate risks

Simple processes and guidelines that don't slow development

- Developers don't want to guess what to do with regards to OSS
- Guess = ignore

Tools or services to manage OSS

 Don't make it harder than it has to be



How do you keep lawyers calm?

OSS audits

 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)

Process for reporting OSS usage

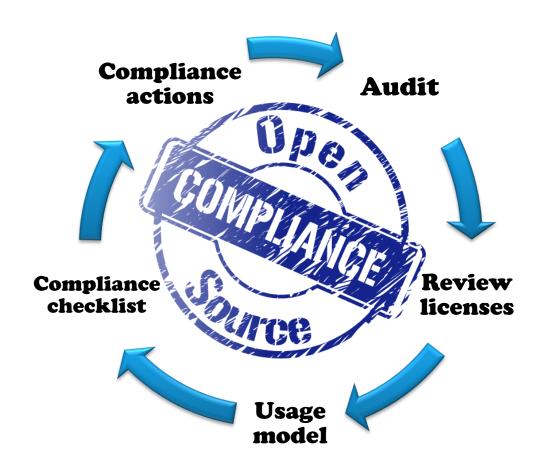
- Make development teams (now armed with their new knowledge of OSS) report all OSS usage going forward as they download
- Delineate based on license types and usage

OSS usage guidelines

- 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





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/linuxtraining-videos#compliance
 - https://training.linuxfoundation.org/linux-courses/open-sourcecompliance-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



Q&A

