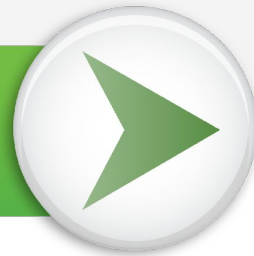


NONE BUT THE BRAVE CAN EAT THE FARE

Avoiding our own “Jungle” of the commercial Software Supply Chain

Justin Rackliffe

Director, Open Source Governance



Who Am I?

- Responsible for Open Source Governance at Fidelity Investments
- Represent Fidelity Investments with Linux Foundation and TODO Group
- Advocating for shared responsibility in doing great things with OSS



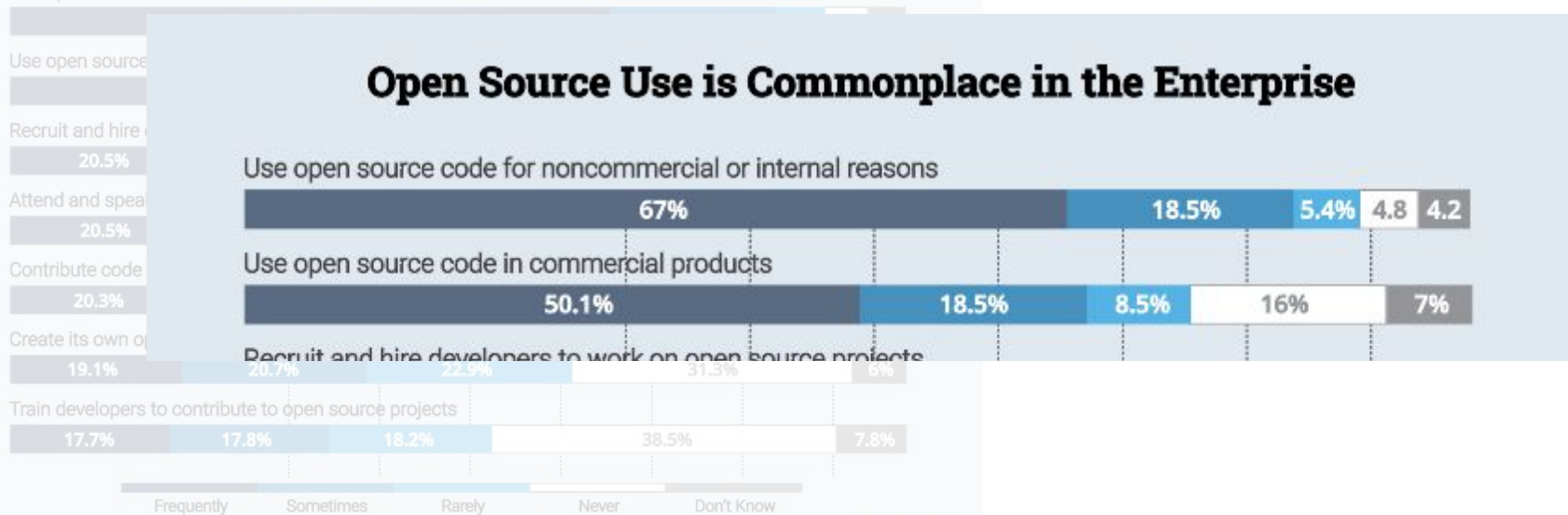
How could they find out that their tea and coffee, their sugar and flour, had been doctored; that their canned peas had been colored with copper salts, and their fruit jams with aniline dyes?

- Upton Sinclair, *The Jungle*

TODO Group Survey 2019

Open Source Use is Commonplace in the Enterprise

Use open source code for noncommercial or internal reasons



Source: "Open Source Programs in the Enterprise - 2019" Survey. Q: How often does your company do the following activities? n=2652.



Life comes at you fast

The screenshot shows the website 'the npm blog' with a red banner for 'The Register' and the tagline 'Biting the hand that feeds IT'. The navigation menu includes CORONAVIRUS, DATA CENTRE, SOFTWARE, SECURITY, DEVOPS, BUSINESS, PERSONAL TECH, and SCI. A blue sidebar contains social media icons for Facebook, Twitter, and YouTube, along with a search bar and a menu with items like 'ISSUE REMOVAL GUIDES', 'TUTORIALS', and 'DEALS'. The main content area features a headline: '(* SOFTWARE *) What happens when the maintainer of a JS library downloaded 26m times a week goes to prison for killing someone with a motorbike? Core-js just found out'. Below this is a sub-headline: 'Backdoored Python Library Caught Stealing SSH Credentials'. The author is listed as 'By Catalin Cimpanu' and the article is dated 'May 9, 2018' at '05:07 AM' with 1 comment.

What can be done?!

- Basic knowledge around open source licensing and lifecycle
- Be curious and sensible around your partnerships
- Use the power of purse and policy

We need to expect more of our suppliers so that there are the required motivations in the marketplace to establish a new normal

Expecting More

- Attribution Notices
- Blackbox Manifest Analysis
- Exception Processes

Attribution Notices

1. Many OSI licenses require it
2. Responsiveness indicates awareness
3. Security by obscurity



Blackbox Manifest Analysis

Given an attribution notice you may be able to get a very rough idea of possible gaps in a partner's processes.

npm audit

```
{"dependencies": {  
  "npmname1": "version",  
  "npmname2": "version",  
  "npmname3": "version"  
}}
```



bundle audit

```
source 'https://rubygems.org'  
gem "gemname1", "version"  
gem "gemname2", "version"  
gem "gemname3", "version"
```



safety

```
pipname1==version  
pipname2==version  
pipname3==version
```

Exceptions

- Starts with a Policy
- Operating under Exception is not comfortable
- Defining and Accepting Risk
- Remember you are the one with the money

Summary

- Risk appropriate Policies
- Lack of context make all problems simple
- Interest will drive investments by everyone
- Goal is a conversation driven by information



<https://www.coreinfrastructure.org/programs/census-program-ii/>



<https://clearlydefined.io/about>

*We sit at a table delightfully spread,
And teeming with good things to eat.
And daintily finger the cream-tinted bread, Just needing to make it complete,
A film of the butter so yellow and sweet, Well suited to make every minute
A dream of delight. And yet while we eat, we cannot help asking “What’s in it?”*

- Harvey Wiley, "I Wonder What's In It"
The Poison Squad, American Experience