NONE BUT THE BRAVE CAN EAT THE FARE

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

Justin Rackliffe
Director, Open Source Governance

Fidelity INVESTMENTS

Who Am I?

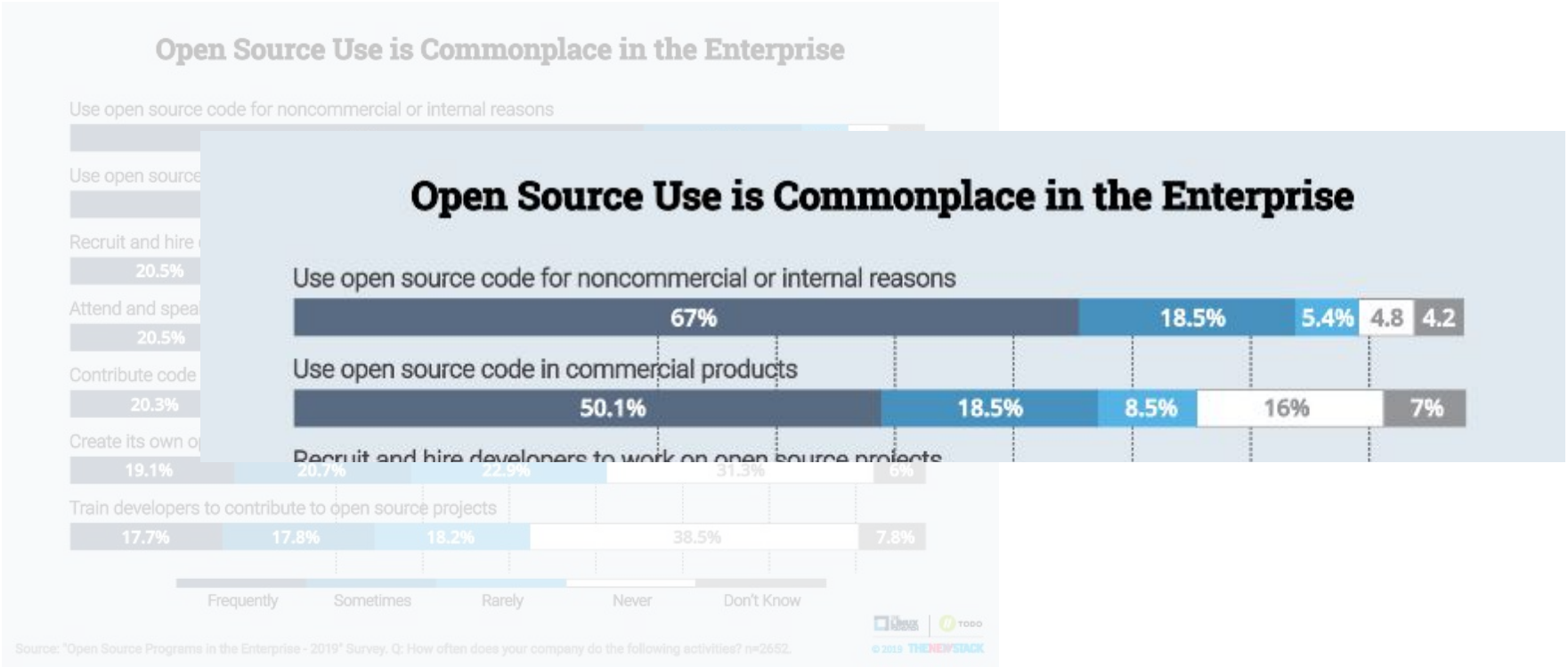
- Responsible for Open Source Governance at Fidelity Investments
- Represent Fidelity Investments with Linux Foundation and TODO Group
- Advocating for shared responsibility in doing great things with OSS

Fidelity INVESTMENTS

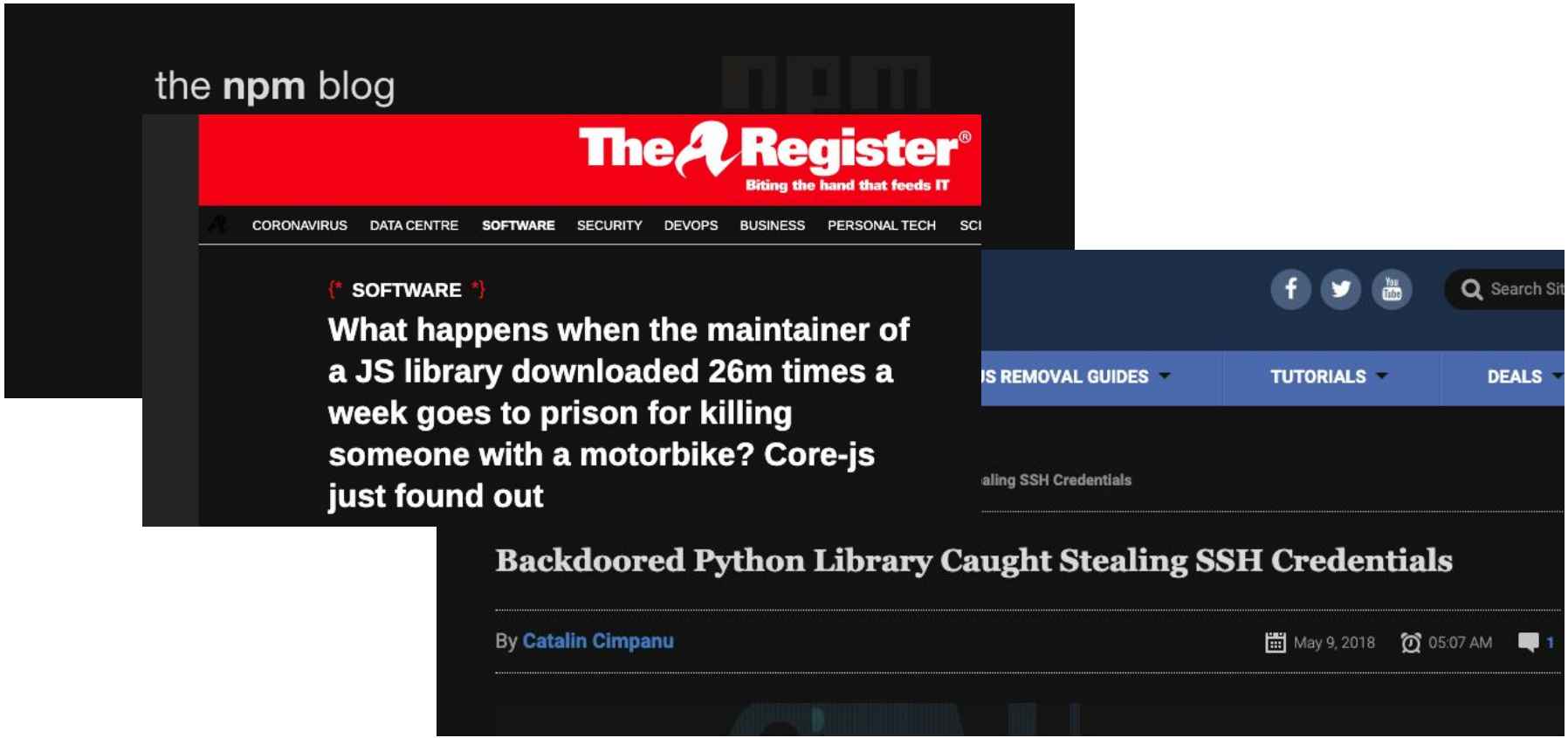
How could they find out that their tea and coffee, their sugar and flour, had been doctored; that their canned peas had been colored with copper salts, and their fruit jams with aniline dyes?

- Upton Sinclair, The Jungle

TODO Group Survey 2019



Life comes at you fast



What can be done?!

- Basic knowledge around open source licensing and lifecyle
- 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

Fidelity INVESTMENTS

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