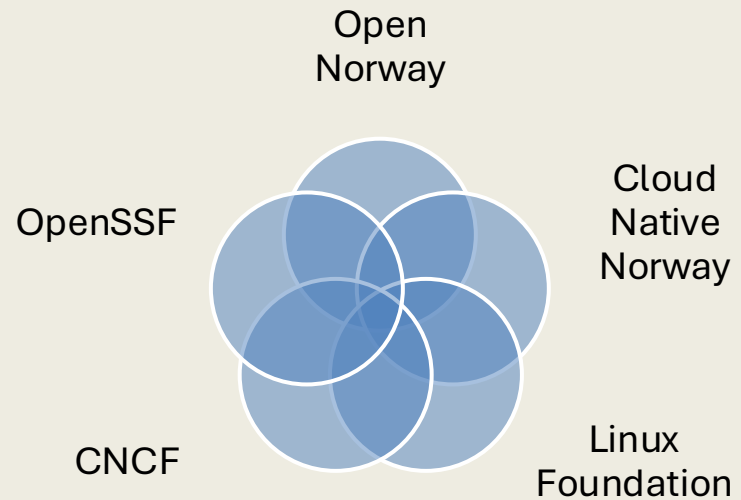


**Take your company from passive
consumers to active contributors**

Roberth Strand

Senior Manager @ Sopra Steria

Microsoft MVP & CNCF Ambassador



FOSS will always be the foundation, and it is important to have a good foundation.

What we'll cover

- The reality: how much of what you ship is already open source
- Maintainer burnout: the hidden risk
- Why contribute: the business case
- Building the OSPO: strategy and guardrails
- Getting started

Open source is the foundation you're already standing on

96%

of commercial codebases contain open source.

\$8.8T

the cost to rebuild it all from scratch.

Source: Hoffmann, Nagle & Zhou, "The Value of Open Source Software," Harvard Business School.

When the foundation cracks, you inherit the risk

- **xz-utils backdoor (CVE-2024-3094)**: a compression library in nearly every Linux distro, maintained largely by one volunteer.
- A years-long social engineering campaign exploited that burnout to slip a backdoor into the build: caught by chance, days before it shipped.

“The burden of security shouldn’t fall on an individual open source maintainer.”

— CISA, *Lessons from XZ Utils*

xz-utils wasn't a one-off

Log4Shell: CVE-2021-44228 (2021)

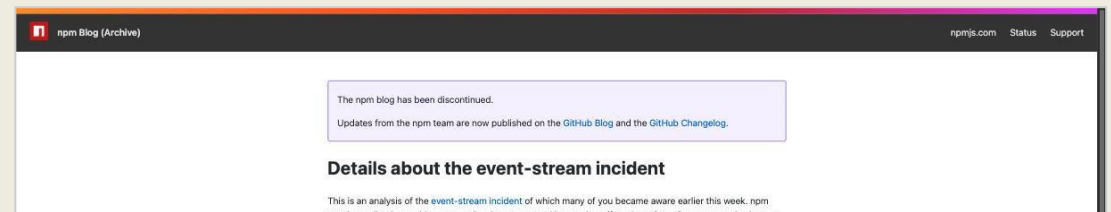
A single flaw in Log4j, a logging library embedded almost everywhere in enterprise Java, let attackers run arbitrary code on millions of servers overnight.



Source: CISA, joint Cybersecurity Advisory AA21-356A, "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities" (Dec 2021).

event-stream (2018)

A volunteer maintainer, worn down and glad for the help, handed commit access to a stranger: who quietly shipped code built to drain cryptocurrency wallets.



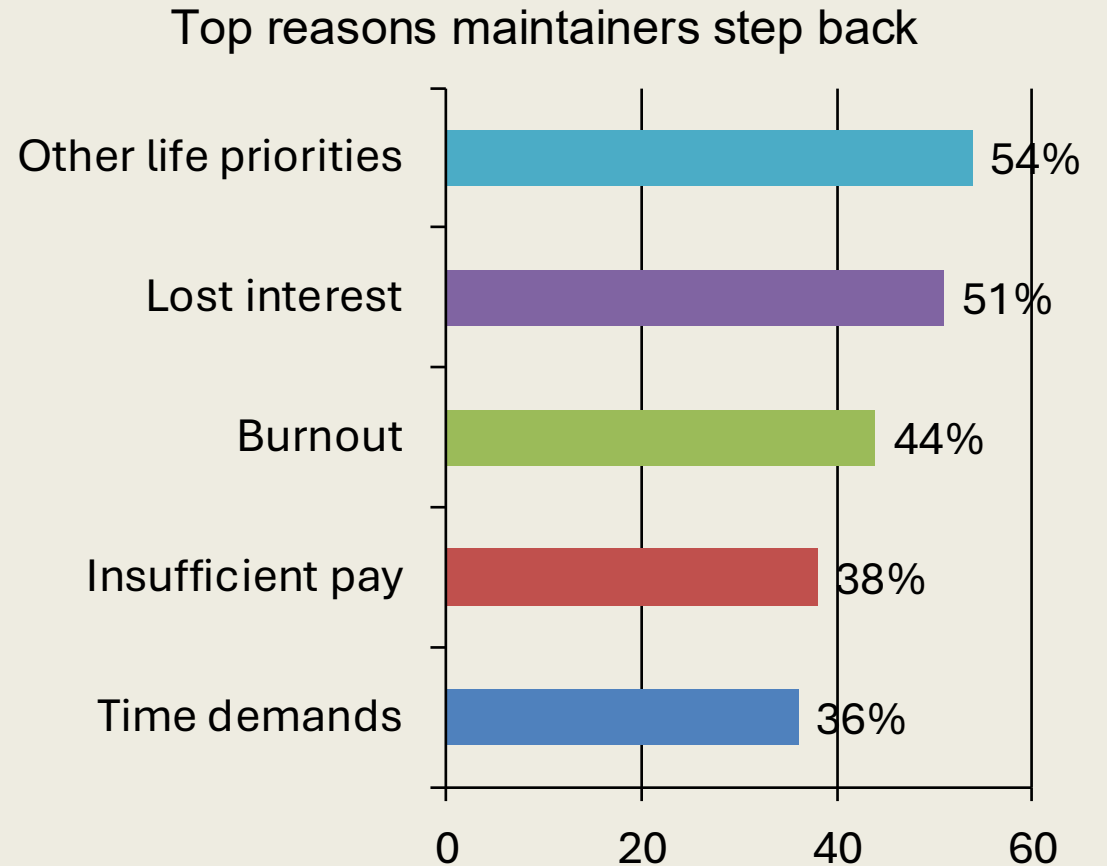
Source: npm Blog Archive, "Details about the event-stream incident" (Nov 2018).

Burnout is a supply chain risk

58%

of maintainers have quit, or considered quitting, a project they maintain.

Source: SonarSource / Tidelift maintainer survey.



Contribution turns dependency into advantage

- **Shape the roadmap:** influence, before it ships
- **Get fixes faster:** no more private forks
- **Attract talent:** engineers want this
- **Stronger security:** more eyes on the code

2–5x

the ROI companies see from actively contributing to open source.

Source: Linux Foundation Research, ROI for Open Source Software Contribution (2026).

Contribution doesn't have to mean code

- **Foundation membership:** join and help steer the projects you depend on
- **Documentation:** fix the docs everyone struggles with
- **Bug reports & feature requests:** a good report is a contribution
- **Share knowledge:** talks, blog posts, forums, meetups

What “dedicating resources” actually looks like

- **Upstream-first policy:** fix it where it lives
- **Named contributor time:** real hours, real work
- **Sponsor dependencies:** fund what you can't lose
- **Executive sponsorship:** visible backing, not a side project

Enter the OSPO

Ad hoc contribution doesn't scale.

An Open Source Program Office is how you turn it into a lasting, funded practice.

Building the OSPO

An OSPO is the team that sets your company's strategy and guardrails for open source.

The guardrails an OSPO puts in place

- **License compliance:** know what you ship
- **Security review:** vet what comes in
- **Contribution policy:** a fast, clear path
- **Governance & brand:** how you show up publicly

This is already normal at scale

- **Google:** AI, cloud & OSS security (OpenSSF)
- **Microsoft:** Kubernetes & supply chain security
- **Meta:** PyTorch, React, GraphQL
- **IBM:** hybrid cloud & Hyperledger
- **Goldman Sachs:** firmwide OSPO since 2021
- **Bloomberg, Comcast, Porsche:** TODO Group's Evolution of the OSPO case studies

Source: TODO Group, Lessons from the Industry's Leading OSPOs; The Evolution of the Open Source Program Office.

OSPPOs mature in stages — start wherever you are

- **0 • Ad hoc:** no policy, no inventory
- **1 • Legal-driven:** licensing and compliance
- **2 • Community-driven:** starts contributing back
- **3 • Engagement-driven:** dedicated staff, real process
- **4 • Leadership-driven:** shapes tech strategy

Source: Open Source Initiative — The Five Stages of the Open Source Program Office.

You don't have to start from zero

- **TODO Group:** the Linux Foundation's vendor-neutral community of OSPO practitioners.
- **The OSPO Handbook (ospobook.todogroup.org):** a free, community-written guide: the value case, creating your OSPO, day-to-day operations, security, metrics, and real end-user journeys.
- **State of the OSPO report:** TODO Group's annual survey of OSPO adoption and maturity, published with LF Research.

Where to start on Monday

1. Inventory what you already use and contribute to.
2. Write a one-page contribution policy.
3. Name an OSPO owner: even part-time.
4. Fund one critical dependency this quarter.
5. Track the impact. Share it.

Four things to remember

- Open source is infrastructure: not a free resource.
- Burnout upstream becomes risk downstream.
- Contribution is an advantage, not charity.
- An OSPO turns intentions into guardrails.

Thank you.

Questions?