EXHIBIT 16

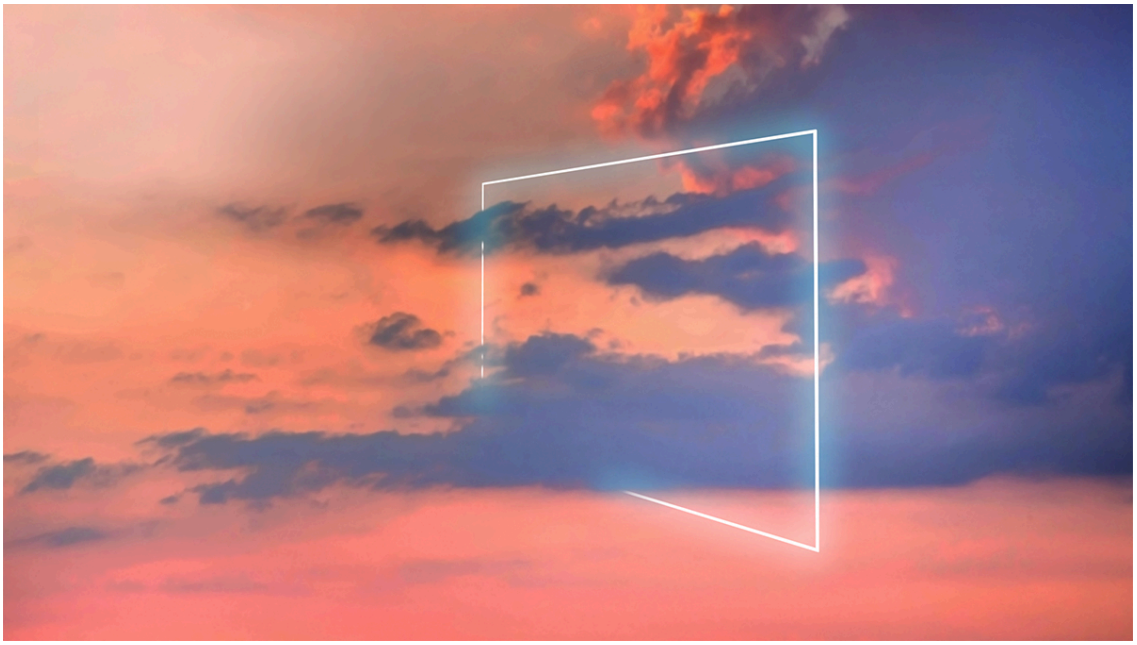
Harvard Business Review

Technology And Analytics

The Digital Economy Runs on Open Source. Here's How to Protect It.

by Hila Lifshitz-Assaf and Frank Nagle

September 02, 2021



Artur Debat/Getty Images

Summary. Free and open source software (FOSS) is essential to much of the tech we use every day — from cars to phones to planes to the cloud. While traditionally, it was developed by an army of volunteer developers and given away for free, companies are increasingly taking... **more**

Though most people don't realize it, much of the technology we rely on every day runs on free and open source software (FOSS). Phones, cars, planes, and even many cutting-edge artificial

intelligence programs use open-source software such as the Linux kernel operating system, the Apache and Nginx web servers, which run over 60% of the world's websites, and Kubernetes, which powers cloud computing. The sustainability, stability, and security of these software packages is a major concern to every company that uses them (which is essentially every company). But unlike traditional closed-source software, which companies build internally and sell, FOSS is developed by an unsung army of typically unpaid developers, and is typically given away for free.

In the last few years, we have observed an increase in the active role of corporations in open source software, by either assigning employees to contribute to existing open source projects or open sourcing their own code both to allow the community to utilize it and to help maintain it. As companies have made FOSS part of their business model, they have also acquired important FOSS producers. Two years ago, IBM purchased Red Hat, one of the most successful companies built around FOSS for $34 billion. A year before that, other tech giants paid billions to acquire a stake in FOSS, most notably Microsoft (bought GitHub for $7.5 billion) and Salesforce.com (bought MuleSoft for $6.5 billion).

The corporate world's entry into free and open source online communities has caused some serious concerns and friction. Acquisitions of FOSS producers could lead to a crowding-out of volunteer contributors to an extent that threatens the future health of the FOSS ecosystem. Further, the world's largest cloud providers have built multi-billion dollar businesses on top of FOSS components, leading FOSS contributors to wonder why they are spending their free time making the rich richer. Such actions can deter volunteers from contributing, threatening the underlying ethos of the FOSS community.

One particularly contentious case is the recent conflict between Elastic vs. Amazon. Elastic, a public company whose Elasticsearch software powers search activity on numerous corporate websites like Walmart and Audi, battled with Amazon after the online giant took a version of Elasticsearch that Elastic had made open source, repackaged it, and sold it to their customers under nearly the same name. Elastic argued that essentially Amazon took free code that created value for the whole community, and walled it off so that they were the only ones who could capture value from it.

With the support of the Linux Foundation and in conjunction with the cross-industry Open Source Security Foundation, we have undertaken two complementary research efforts — one focused on conducting a census of FOSS usage and the other on understanding FOSS contributor motivations — seeking to better understand these concerns. For the first, we partnered with software composition analysis and application security companies, including Snyk and Synopsys, to gain broad insights into FOSS usage in production applications by conducting a census of this critical software to identify the most widely used FOSS packages. For the second, we performed a large-scale global survey of the FOSS developer community that asked why developers contribute to specific FOSS projects, how they perceive the significant financial investments from companies, and what security practices they utilize (a considerable issue in FOSS). Here's what we found.

Concerning Findings

The biggest question regarding the increasing involvement of corporations with FOSS is whether it will negatively impact the future health and well-being of the FOSS ecosystem. Will the developers who create the software we all rely on stop participating in a system that is driven less by a sense of community, and more by the pursuit of profit? Will companies focus exclusively on the profitable FOSS while ignoring other

critical pieces of the infrastructure society depends on? Will it be harder to maintain the security of this software? If more of the work on FOSS is done by individual companies, will there be fewer eyes looking for bugs and potential vulnerabilities? If the answer to any of these questions is yes, that bodes poorly for the future of open source software.

The preliminary results of our census reveal two concerning trends that could make FOSS more vulnerable to security breaches. First, we found that many of the most widely used FOSS packages in commercial software are housed under the accounts of individual developers (rather than broader communities), raising the issue not only of security, but also of reliability. An individual may take a new job, may decide to retire, or — fortune forbid — get hit by the proverbial bus and become incapable of maintaining the project. Individual accounts also may not have sufficient safeguards to prevent potentially dangerous attacks from hackers. Second, we found that many companies are using outdated versions of open-source programs — a worrying, if not necessarily surprising finding. Failing to stay abreast of updates means it is more likely the software contains known bugs and security weaknesses. Both trends reflect that security is often an afterthought.

The survey results also revealed that contributors' motivations may require companies to use non-traditional incentives. Although increasingly contributors are sponsored by companies, these contributors primary motivator is not money. This means that corporations' traditional levers for incentivizing behavior may not work, and more intrinsic motivations including the passion for learning, a sense of belonging to the FOSS communities and the professional identity of programmers may need to be relied upon. Therefore, any companies, organizations, or governments looking to enhance the security of FOSS would need to focus on appealing to these intrinsic motivations, rather than just paying contributors to work on security. Alternatively,

companies could pay hired guns to specifically work on security issues. Either way, our survey reveals that expecting contributors to voluntarily address security issues is unlikely to succeed.

How Companies Can Help

No one, certainly not us, is suggesting that we must go back to the early days of FOSS, when it was mostly a voluntary effort by like-minded individuals. But we do recommend big players like companies and governments — which are increasingly sponsoring FOSS both directly and indirectly — to understand the impact they have on the future of the FOSS ecosystem and follow a few guiding principles.

First, the goal of both companies and countries should be to strike the right balance: to see that FOSS continues to grow without snuffing out the community spirit that has been at the heart of the motivations to contribute. This means, companies should have a clear policy towards open source (preferably one that encourages employees to contribute to FOSS if feasible). Our research found that many employees do not have a clear understanding of their company's FOSS policies, which makes them hesitant to openly use and contribute to FOSS projects. Further, they can proactively support these projects to ensure their future health.

Second, companies that use FOSS (which is essentially all companies, whether they know it or not) should raise their level of awareness about the FOSS that they use. A recent presidential executive order requires a software bill of materials (SBOM) be provided for any product purchased by the government so that it knows what FOSS (and proprietary software) is included in the product, and therefore can be aware of potential vulnerabilities that arise. This is an important example that all companies should consider following. Doing this would allow companies to better

understand their reliance on the FOSS community, and would yield more transparency and allow them to know when they are susceptible to newly found vulnerabilities.

Third, as companies continue their involvement in contributing to FOSS, we suggest they keep the stability of the software they use in mind, that they incentivize their employee contributions to focus on both features useful to the company as well as general security and maintenance, and remain cognizant that the volunteer community behind these projects is critical and should be protected. In this way, they are not only gaining from the new features they are adding, but are ensuring the future health and well-being of the FOSS they rely upon.

Free and open source software is a vital cog in the economy, much like interstate highways, the power grid, or the communications network. Given how much we already know about those critical infrastructure systems, doesn't it only make sense to learn just as much about their 21st century equivalent? With the number of stakeholders involved in the FOSS ecosystem, it is difficult for any single actor to solve all of the issues. Thus, it is likely that a multi-party effort including companies, governmental organizations, and individual contributors will be necessary to ensure the security and vitality of the FOSS ecosystem in the future. However, understanding the scope of the problem must occur first. We believe that our efforts are one of the first steps in that direction.

Author's note: If you would like to learn more or get involved, you can read the report on the survey results, or read the preliminary report on FOSS usage and sign up to participate in our next contributor survey, or get involved in the initiative.

HL

Hila Lifshitz-Assaf is an Associate Professor of Technology, Operations and Statistics at NYU Stern. See Hila's faculty bio here.

FN

Frank Nagle is an assistant professor at Harvard Business School where he studies and teaches topics at the intersection of technology and strategy. Previously, he worked in the cybersecurity field for nearly a decade.