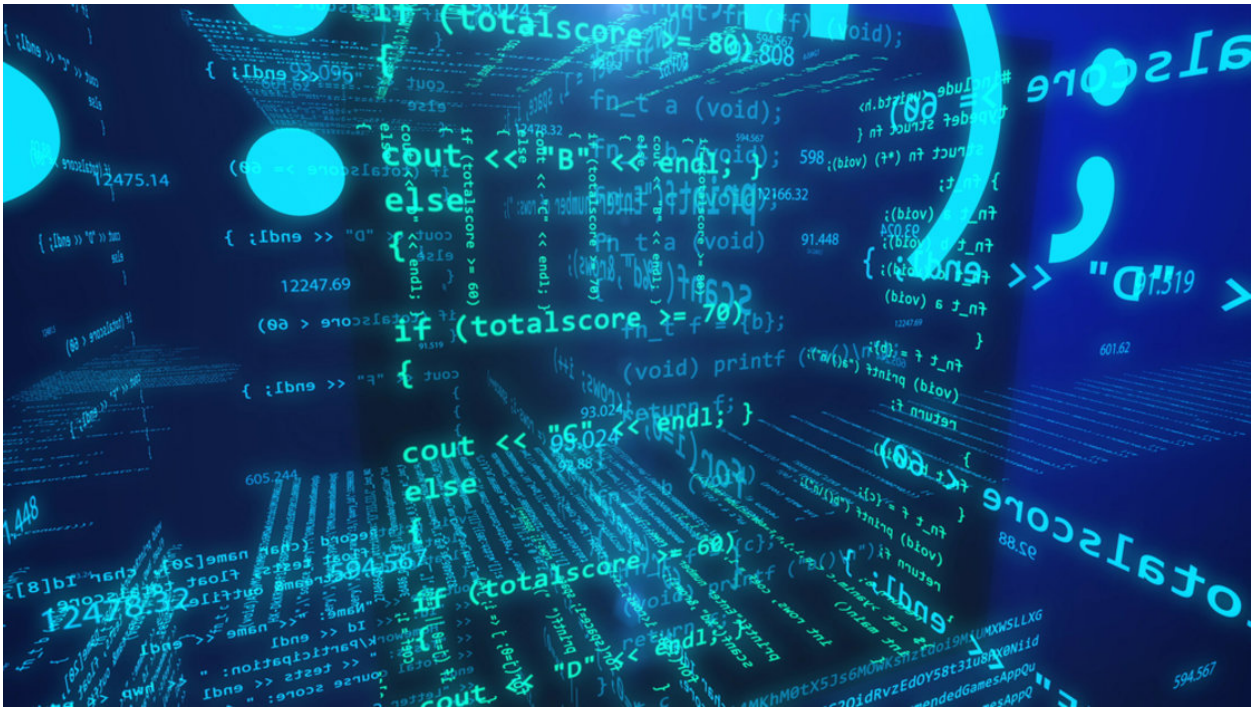
Four Myths About Open Source in Government (Contributed)

David Egts | December 20, 2018



Every year, the National Association of State Chief Information Officers (NASCIO) publishes its list of State CIO Top 10 Priorities, a checklist of the most important issues that will be on the to-do lists of CIOs across the country. This year's list includes concerns about security and risk management, implementation and deployment of cloud services, and the need to consolidate and optimize services and infrastructure, to name a few.

State CIOs may wish to consider turning to open source software for help in addressing these challenges and objectives. Open source can facilitate more flexible and agile IT infrastructure and is the underlying technology behind many popular cloud service platforms. Open source can also help organizations consolidate and centralize disparate services, making them easier and more cost-effective to manage.

Many states and cities are actively embracing open source. California's Government Operations Agency recently launched the California Code website, an open collaboration between agencies, industry partners and civic technologists working to create a more innovative, collaborative and effective government. The state has also certified the first open source, publicly owned election technology for use in Los Angeles County. Meanwhile, in Chicago, open source has been embraced by the Office of Budget and Management (OMB) to simplify and modernize the city's annual financial reporting obligations. Yet, despite its many benefits, myths about open source persist.

Here are four persistent misconceptions about open source and tips on how government organizations can discern myth from reality to advance their mission.

Myth #1: Open Source Is Totally Insecure

The first persistent myth is that open source software isn't as secure as proprietary software. After all, security through obscurity is poor security. The transparent nature of open source creates a vested interest for code developers and vendors to respond quickly to vulnerabilities through constant peer review. Unlike proprietary software, open source code is often developed in collaboration and shared across communities (including government and financial services sectors), so that any security flaws can be addressed quickly.

Myth #2: Open Source Is Totally Secure

Pivoting from alarm about potential security issues, a new concern has emerged, and it's a valid one — that open source is inherently more secure. And it's a myth that we must dispel. Just because the code is transparent and visible to all, it is not, as many assume, secure by default. Not all open source developers have the time, interest or skills to do security — which could leave government exposed to vulnerabilities. Without an active and vibrant community, it falls to the open source consumer to do their own due diligence — to identify potential security flaws and respond accordingly.

Consumers can also layer in security metrics and health indices published by open source vendors and use third-party tools.

Myth #3: Open Source Software Is Free

To understand why free software isn't free, we should consider the meaning of "free" and how it has evolved with time. Open source as " free software" — i.e., no costs associated — was a key tenet from the beginning. However, for purists open source also exemplified freedom. The freedom to access, change, and distribute source code.

Over time, "free" took on new meaning. In 2005, Sun Microsystems co-founder Scott McNealy coined the term " free like a puppy is free," referring to the long-term costs and responsibilities of so-called "free" open source projects. McNealy was right. You can't blindly download source code and expect it to maintain and patch itself.

More recently, a new analogy lends another perspective: " free as in a mattress." An abandoned mattress on a street is there for anyone's taking. But without knowing where it came from or who's used it, would you take it home? The same is true of open source code. Without information about the supply chain — who wrote it, how secure it is, if it's still maintained — you really shouldn't be using it. With an increased focus on cyber-risks inside government supply chains, knowing the lineage of your hardware and software is critical.

Myth #4: Open Source Participation Is Only for Startups

Although open source software consumption in government is strong, the next phase is for agencies to contribute to the projects they care about most. Public-sector developers

that contribute to open source communities can reap significant benefits. For example, federal, state and local initiatives such as Code.gov and California's Code.ca.gov are using the power of code sharing and collaboration to help government cut down on duplicative software development and save taxpayer dollars.

Unsurprisingly, code reuse is a prime use case for how open source is supporting the efficient use of public funds and resources. Making code developed in one state or municipality available for statewide or nationwide reuse can reduce duplicative costs and efforts for similar projects. The dollars spent building an open source community around a project and encouraging contribution can ultimately pay for themselves, since the investment is shared with like-minded agencies in the U.S. and globally.

Best Practices for Government

As open source adoption grows in government, agencies must be deliberate in their open source strategy. Careful consideration must be given to several factors, such as how transparent and secure is the supply chain? And because there's no such thing as " free," how will agencies pay for support? Should they pay a vendor or staff the support themselves?

Finally, agencies should not be afraid to contribute to open source communities. Thanks to their influence, vendors can also help with this, freeing government staff to focus on the mission. Even those who choose to work independently of a vendor can benefit by choosing open source software that is backed by a vibrant community and participating in it.

Open source myths are persistent, so as you encounter them don't be deterred. A better approach may be to explore these myths, understand what they mean to your agency, and make informed decisions based on research.

http://www.govtech.com/opinion/Four-Myths-About-Open-Source-in-Government-Contributed.html