

A STRATEGY PAPER WITH INSIGHT FROM

CENTER FOR
DIGITAL
GOVERNMENT

Open Source Open Government

An Executive Guide

to Making Strategic Decisions

about Open Source Software

in Public Sector Service

Delivery





Introduction: Open Source as Strategic Inflection Point

PREFACE

Open source software has gained considerable prominence through a debate which is not of its making. It has been cast as the underdog in what some have characterized as a head-to-head match-up with Windows.

One of the competing camps contends that open source is not a story without Microsoft. That is, it argues that the headline, "The City of Munich Chooses Open Source ..." is not news without the final two words "over Windows." This adversarial model has spawned competing claims over the total cost of ownership, functionality and security.

This strategy paper takes the other view - that open source is a strong story on its own merits, based on a unique collaborative history and a promising trajectory in both the private and public sectors. Such an approach avoids the pitfalls that are common in the technology industry where everything is cast in opposition to the dominant industry player of the moment.

Open source is also helping to revise long-held conventional wisdom. In an earlier era, careers were built on the axiom, "Nobody ever got fired for buying IBM." Now, the new imperative is more properly put this way: "Nobody ought to get hired without being conversant about open source."

Open source software has emerged as an overnight sensation that was at least 35 years in the making. The Internet was developed on an open source operating system¹ in the late 1960s when the network of networks was a government protectorate. Over the intervening decades, the Internet has evolved into the world's largest, most complex and most reliable system, serving as a proving ground for enterprise-level open source computing.

The commodity Internet, a designation that reflects the public network's transition from a government protectorate to a commercial concern, represents the defining moment of the last decade – or what Intel founder Andy Grove calls a strategic inflection point, which he defines as, "a change so powerful that it fundamentally alters the way business gets done."²

Open source is well positioned to be a strategic inflection point in the decade ahead – public domain software that forces fundamental changes to the practices of the commercial software industry and the software costs for technology users. This inflection point comes as the open source movement, nurtured by a loose knit community of software developers, becomes mainstream, with a burgeoning number of enterprise-scale users supported by a growing segment of the technology industry that is investing heavily in making open source ready for prime time.

¹The Internet relies on Transmission Control Protocol / Internet Protocol (TCP/IP), which originated as open source and has since been commercialized in a broad range of applications. Source: Donald K. Rosenberg, *Open Source: The Unauthorized White Papers - 1st edition*, John Wiley & Sons, 2000: 37.

²Andrew S. Grove, *Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company - 1st edition*, Currency Publishing, 1996.

TOWARD A CRITICAL MASS OF OPEN SOURCE IN THE PUBLIC SECTOR

The inflection point is also a function of a bruising public-sector revenue recession that has caused government leaders to make tough choices about the allocation of scarce taxpayer resources. To that end, there is a renewed interest in the cost of delivering government services — and a determination to change the cost structure of operating government, particularly those things that are done commonly across agency or jurisdictional lines.

The free distribution of open source software has been a determining factor in the choices of governments in Australia, Brazil, Canada, China, Germany, India, Spain, and Thailand to use open source in mission-critical computing. The U.S. Department of Defense and Treasury Department have done likewise, and the General Service Administration has created a registry of common open source software components. Among political subdivisions in the United States, the commonwealth of Massachusetts is founder and anchor of the Government Open Code Collaborative, a registry shared with Pennsylvania, Utah, Missouri, and Rhode Island among other state and local governments. The registry makes real a concept long advocated by the National Association of Chief Information Officers (NASCIO) to optimize use and re-use of software developed to do the public's business. At the same time, state governments in California, Oklahoma, Oregon, and Texas have recently taken steps to encourage agencies to use open source software in their development efforts.³

The purpose of this strategy paper is to provide context for deciding whether and how to consider the role, if any, of open source in government organizations. This guide for “fast followers,” a term made popular to describe a strategy of pioneering after explorers have cleared the path, comes in five essential parts:

- 1) A common plain English definition of open source;
- 2) A brief policy discussion of the consistency of the animating principles behind open source and open government;
- 3) An overview of the origins of open source and the community of software developers who created the evolving code base;
- 4) The implications of the commercialization of open source implementations; and
- 5) The outlines of a management framework for making sound business decisions about adopting open source for the mission-critical work of government.

OPEN SOURCE IN GOVERNMENT: A DEFINITION

It is useful to work from a common definition in the discussion that follows:

Open Source in Government (*noun*): A community-developed, non-proprietary code base that brings with it the promise of cost effectiveness, more rapid development, and flexibility in applications for doing the work of government.

Although most of the open source code base is free for the taking (subject to certain license restrictions), open source is not different because it's “free” (after all, there's nothing illegal about charging for it). Open source is different because the code is out in the open where developers can freely see and comprehend it.

With full access to the underlying source code, developers can modify it to meet the needs of a specific organization more quickly, which increases productivity of the organization while the continuing work of the wider open source community addresses bugs and bad code — thereby increasing the stability of the underlying open source product.

The open source kernel is at the core of

an operating system that runs machines, applications that deliver business functionality and software objects or modules with which they are built. Each of the three have enjoyed considerable growth in adoption among institutional users.

Operating Systems: Servers operating on open source accounted for a 16 percent share of the market in 2003, which is expected to grow to 30 percent by 2008.⁴ At the desktop, an open source-on-Intel platform is projected to grow five to 10 percent by 2009.⁵

Applications: By one estimate, there are 80,000 known applications developed and deployed using open source.⁶

Objects: There are at least 70,000 open source components available on the Internet for download such that smart developers can create new applications faster and cheaper.⁷

The critical need to operate effectively amid crushing cost constraints provides a substantial incentive to use open source software to replace proprietary products used to provide those functions that are common to all organizations — ranging from routine functions such as file, print, messaging, and Web server to more advanced applications related to business functions — within government and without. One open source distributor correctly noted, “While systems must reliably perform these functions, it makes little sense to spend any more than absolutely necessary to maintain this functionality, not when those funds can be better spent on new development that will provide specific strategic or tactical advantage.”⁸ Obviously, open source can be used to develop non-common functionality too, but with diminished prospects for sharing and reuse.

POLICY: OPEN GOVERNMENT AND OPEN SOURCE

In the United States, federal, state and local governments have been forced open by hard-fought victories in their

³True to open source's origins as a movement, there have also been grassroots efforts to encourage government's use of open source in Alabama, Hawaii, Iowa, and Louisiana.

⁴IDC Research, 2004. ⁵Forrester, 2004. ⁶SourceForge, 2004. ⁷NASCIO, Forrester. ⁸Creative Commons, 2004.



respective legislatures or directly at the ballot box through citizen initiatives. The continuing campaign for open records and open meetings are intended to make the inner workings of government transparent. Consider the similarities with the drive for open systems, which was intended to ensure maximum interoperability and best use of scarce taxpayer resources.

While open government and open source attract different proponents and opponents with widely different motivations, both are driven by turf. On the one hand, open government is about who controls access to public records and under what circumstances. On the other hand, open source in government is about the circumstances under which public domain software is used in concert with (or to the exclusion of) proprietary code. Still, there is a natural fit between open source and open government in that both encourage a greater range of options or choices, while putting a premium on information sharing, transparency and, ultimately, public accountability.

ORIGINS: IT TOOK A VILLAGE TO CREATE THIS CODE BASE

The open source code base has been developed and is being perfected by a networked community of developers, the members of which came of age on the Internet. Open source software is perhaps known by the proper name of one of its most used kernels: Linux. Originated by namesake developer Linus Torvalds in 1991, Linux offered a “no name” equivalent of the robust Unix operating system at a considerable cost advantage. Linux has emerged as the main driver for open source, and is arguably the open source technology most used in the public and private sectors alike.

From the start, Linux was designated as open source. (In fact, the Linux kernel itself was built largely by tools licensed under the dominant open source licenses, and the complete Linux

operating system consists of many utilities and applications likewise licensed as open source.⁹) Moreover, with Linux as open source, it meant that (a) the underlying source code was transparent for developers to see, comprehend and build upon; and (b) contributions are allowed from anywhere by anyone. As author Donald Rosenberg writes in *Open Source: The Unauthorized White Papers*, “Under the open source model, community-based development is used. That is, most open source applications are developed through the contributions of many (sometimes thousands) of contributing volunteer developers.”¹⁰

The result is a collaborative ecosystem intended to attract developers with the greatest skill and expertise to perfect the product. While the community-based collaborative development model may allow errors originally, it is self-correcting in that robust peer review weeds out bad code. The community that created the code base, and perfects it through continuous improvement and peer review of new components, has been bolstered by commercial interests who have embraced open source as a neutral place to start again after the platform wars of the last decade.

Unlike proprietary operating systems, the open source ecosystem developed around a common Linux platform to advance hardware drivers, improve security and create IT skills that work across a variety of IT jobs.

To be clear, running open source does not isolate your organization. For the most part, Linux on the desktop looks, feels and acts much like commercial productivity products. At the server level, an open source operating system is virtually indistinguishable from its commercial counterparts on the Internet, thanks in large measure to the open standards that tie the network of networks together. And Linux partitions on mainframes extend the value of existing investments in big iron at only marginal cost.

⁹Rosenberg, 90. ¹⁰Ibid., 2.

FUTURE: IT WILL TAKE TRUSTED PARTNERS TO COMPUTE IN THE OPEN

“A trend towards Linux will tend to pull the market together, making more application software available across more devices”

-From *Open Source*:

The Unauthorized White Papers

The open source community is reshaping the software industry, breaking decades of dependence on proprietary, closed systems in favor of open systems running on open source. By definition, no organization “goes it alone” in the open source community – each is expected to be both a user of and

contributor to the code base. Moreover, many organizations confront open source with vast sunk investments in closed systems, resulting in hybrid strategies to reconcile the installed base at the core with open source at the edges.

The good news is that there is an opportunity to adapt the mature disciplines of computing on the raised floor to the relatively nascent practices of open source at the enterprise level. The bad news is that the introduction of open source can further strain the already strained resources and expertise of most

IT organizations.

For those organizations considering open source, it’s worth asking whether the collaborative instincts needed to be successful are a dominant gene in government or if it is more like being left handed in that it is relatively rare and requires different thinking.

If such skills are rare in a given organization, there is help – often from technology companies with which it may already be doing business. Indeed, the IT services sector (almost all the big names you know) is recalibrating to offer applications, systems, hardware, and third-party, fee-for-service support for specific open source products that are enterprise-ready.

The industry has invested over \$1 billion on the commercialization of open source

to upgrade the code for enterprise-level general business, data-center and telecommunications purposes. Industry players are converging on a model of recurring licenses, support contracts and consulting services for open source software that gives their proprietary software an inexpensive platform to ride on, is pre-loaded on their hardware, and extends the value of legacy systems by maintaining and optimizing them. Under this new model, Linux vendors typically build Linux into so-called “distributions,” which are compilations of free software built around the Linux kernel and sold for a fee with or without accompanying maintenance agreements.

The tricky balance point for industry: Make open source safe for mission-critical computing, while keeping costs down in ways that are attractive to their installed base of users, as well as prospects for a pure play open source.

In surveys of software developers, the research company Evans Data reports that fully 92 percent of respondents claimed that their Linux machines had never been infected by malicious codes, and fewer than seven percent said that they have been the victims of three or more hacker intrusions. Evans also reports that over three-quarters (78 percent) of developers have never been hacked, almost double the rate of developers on other platforms.

The resistance to malicious codes and hacking cannot be attributed to the obscurity of Linux applications. The London-based research firm mi2g Intelligence says that Linux emerged as the most attacked server-side operating system in February 2004 compared to Windows at 22 percent, which remains the largest attack surface in cyberspace.

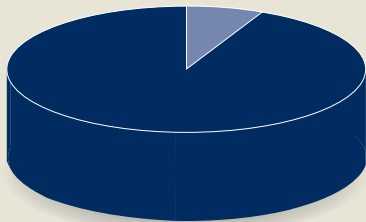
Vital Security Statistics from an Open World

Virus Resistant

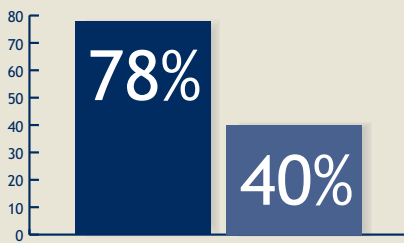
92%

Linux Systems Never Infected

Source: Evans Data



Never Been Hacked

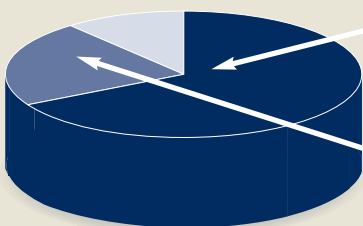


Linux Developers

All Other Developers

Source: Evans Data

Attack Attempts



67%

Linux Systems

22%

Windows

Source: mi2g Intelligence

A Growing Critical Mass of Open Source in Government

The Massachusetts-based Government Open Code Collaborative provides a shared registry for seven states and four municipalities.

The U.S. Department of Defense uses open source for encryption, fire walls and e-mail list management.

The U.S. Treasury Department relies on OSOS for tax collection, accounting and budget management. (Source: George Washington University)

The U.S. GSA is developing CORE to have a registry of common objects for its discovery, development, improvement, and reuse.

Governments in Australia, Brazil, Canada, China, Germany, India, and Spain have all implemented mission critical OSOS.

MANAGEMENT: AN OPEN MIND ABOUT OPEN SOURCE

Open source has gone from a back office passion of a select few to an architectural element that has attracted a critical mass of institutional users, forcing attendant changes in the software industry. For many, the cost savings of open source are irresistible, particularly on the heels of a punishing public sector revenue recession during what *Forbes* magazine famously called the “decade of cheap.”

The management decisions related to whether, how and when to choose open source software involves a complex interwoven web of issues, including technological, business and policy choices with particular focus on upfront investments, lifecycle costs, scalability, reliability, and security.

Two recent, but separate, surveys of institutional users are instructive as indicators of how life looks out in the open:

WHY LINUX?

- 1 Reliability
- 2 Acquisition Cost
- 3 Performance
- 4 Security
- 5 Total Cost of Ownership

Source: Computer Associates (CA) (2004) survey of 2,500 enterprise customers

WHY NOT?

- 1 Dependence on Microsoft
- 2 Inertia of Legacy Systems
- 3 Lack of Support
- 4 Image of Open Source
- 5 Lack of Strong Model

Source: Evans Data (2004) survey of 550 developers on the largest impediments to wide scale adoption of open source in their organization

The survey results suggest that the benefits are compelling, but the perceived obstacles can appear daunting. It is noteworthy that, in the case of open source, inexpensive software is also seen by the organizations that use it as high performing, well behaved and reliable.

Decision makers can be excused for harboring concerns about acquisition costs as a double-edged sword. The initial advantages of low- or no-cost acquisition can disappear in the absence of sound system management capabilities. Clearly, to retain cost advantages, open source organizations must develop that capacity, or contract with those providers that have it, such that Linux is easy to install, configure, update, and secure.

Open source’s security advantages, as reflected in the CA poll, will have to be defended against its growing popularity and the attendant risk that comes with being a larger attack surface. At the same time, the commercial software service industry’s new business model, described above, represents an important step in addressing image and support issues identified in the Evans survey.

The decision to pursue open source is not a silver bullet to all that ails an organization. Like any such choice, there is much hard work in making a good decision, and even more hard work in making a success of it.

Finally, in doing due diligence, it may be useful to have two more lists: the five things to expect of a credible supplier or private sector and the 10 things expected of those who lead organizations into the open. Each are annotated with their essential characteristics.

Reasonable Expectations of Credible Suppliers

FINDING A PARTNER IN EARNEST FOR THE OPEN SOURCE JOURNEY

- 1 Indemnification:** You should be held harmless in the legal squabble over proprietary claims of ownership on components of open source.
- 2 Service Level Agreements:** Contractually binding assurances on stability, scalability and security of the systems they are helping you build and deploy.
- 3 Disciplined Support:** Supplier should bring better-than-commercial-software levels of support to bear on open source because you are paying for the quality of service, not the software.
- 4 Hard Core Commitment and Capacity in Open Source:** Given that most organizations lack the bench strength, suppliers should be chosen based on their proven

experience and reliability in deploying open source in public organizations of similar scope, size and mission as yours.

They should be able to provide the services needed to deploy any operating system – migration programs to aid transitions, education programs to assist knowledge transfer and interoperability management to ensure workable exchanges among Linux, UNIX and Windows among others.

- 5 Maintain Cost Advantages:** Add value without doing violence to the cost advantages of computing in the open by excessive fees for service and support, including but not limited to automated management tools to reduce the cost of ownership for Linux.

Leading into the Open

MAKING THE CHOICE, THEN MAKING IT HAPPEN

- 1 Ensure Organizational Readiness:** The new Open Source Maturity Model is a hard-nosed evaluation tool for assessing appropriateness of fit among business and functional requirements; the project team qualifications and capacity; and, the quality and functionality of the open source product.
- 2 Institutionalize a Critical Eye on Development Options:** Develop a disciplined approach to evaluating open source components.
- 3 Do the Math:** Compare the total cost of ownership of integrating, testing and maintaining a system assembled from commercial, home-built and open source components.
- 4 Recruit the Faithful:** Involve the open source devotees already in your IT organization. (They already think and act like the community that created the code base.)
- 5 Practice the Highest Form of Flattery:** Follow worn paths to success in other areas where reuse and sharing actually worked for your organization or one like it.
- 6 Make a Deliberate Architectural Decision:** Determine how open source integrates into your IT architecture or whether open source is your next IT architecture.
- 7 Know the Rules:** Figure out how to procure “free software” under current rules early before a last-minute flag is thrown down on the play from a concerned attorney.

Further, understand the distinctions between the two major licensing regimes for open source.¹¹

- 8 Launch, Learn and Give Something Back:** Allow developers the freedom to experiment, launch and learn, and tell you how a particular project can work best. Remember that free riders are unwelcome in the open source community. Commit to devoting the necessary resources to both contributing to and reusing open source if you want the movement to succeed.
- 9 Beware of Overreaching:** Application or component sharing and re-use makes it easier to do the next thing. Be careful to ensure that the next thing is consistent with the organization’s public mission and does not duplicate services already available from other sources.
- 10 Prepare for the Blowback:** Companies wedded exclusively to proprietary software products will position their projects against the “risks” of open source. Allied industry groups, including but not limited to the Business Software Alliance, Initiative for Software Choice and American Electronics Association, have proven effective at rallying political ire at the prospect or perception that a move to open source may exclude suppliers of proprietary code.

¹¹ The most often used GNU Public License allows users to modify the source code, provided that the modified source code is in turn freely distributed. In contrast, the Berkeley Software Distribution license has no requirement for subsequent distribution.



© 2004 Center for Digital Government
a division of e.Republic, Inc.
100 Blue Ravine Road
Folsom, CA 95630
916.932.1300 phone
916.932.1470 fax

www.centerdigitalgov.com

CENTER FOR
DIGITAL
GOVERNMENT

About Center for Digital Government:

The Center for Digital Government is a national research and advisory institute on information technology in state and local government. Its custom research, reports and whitepapers, online resources, studies, and advisory services are tailored for private and public sector professionals.

Underwritten by:

Novell®

About Novell:

Novell, Inc. (Nasdaq: NOVL) is a leading provider of information solutions that deliver secure identity management (Novell Nsure™), Web application development (Novell exteNd™) and cross-platform networking services (Novell Nterprise™), all supported by strategic consulting and professional services (Novell NgageSM). Novell's vision of one Net - a world without information boundaries - helps customers realize the value of their information securely and economically. For more information, call Novell's Customer Response Center at (888) 321-4CRC (4272) or visit <http://www.novell.com>.

Novell, exteNd, Nsure and Nterprise are all registered trademarks; and Ngage is a service mark of Novell, Inc. in the United States and other countries. All third party trademarks are the property of their respective owners.