Overcoming hurdles to innovation with cloud and open source

BY STATESCOOP STAFF

Government leaders need the help of commercially-supported open source and cloud technologies to help address some of the most pressing challenges facing state and local government today.

State and local government finds itself at a significant inflection point — opportunities presented by emerging technology come alongside challenges that threaten the very delivery of government services and operations.

As leaders attempt to work their way through these challenges and channel their team's efforts into sustainable progress and change, agencies also must consider the processes and technology that will help deliver better services to citizens.

In a roundtable discussion with several C-level state and local government technology officials from around the Washington, D.C., area, hosted at the Red Hat Government Symposium in November 2017, leaders reported that legacy technology, difficulty with change management inside their organization and cybersecurity challenges are the three main hurdles they face when trying to innovate their business practices.

From that discussion, the consensus was clear: cloud computing and open source software has the potential to radically improve the way government does business — as long as leaders and organizations can offer the necessary support.

That support, along with some help from the private sector, could lead to a sea change in government that will radically change agency operations and citizen services.

"I was not a cloud believer about five years back," one government agency chief information officer said during the discussion. "But I became a cloud believer. If the industry keeps on moving that way, there will be a time when vendors will not be doing anything that needs to be kept on site, and that will force [government] to move to the cloud to get that connection back."

But that impetus to transition to the cloud by embracing open source software comes along with three driving factors that will determine how quick the transition can or will occur over the coming years — the need to modernize legacy systems, increase the cybersecurity postures and use of open source technologies to drive better citizen services.

Legacy modernization

In some cases, before government can even consider shifting operations to cloud, agencies need to start by taking stock of what they already have in their operations, one agency tech official said at the roundtable.

"I'm in the process of basically throwing out what we have purchased three years back and not used, but also figuring out how to use what we have," the CIO said. "The environment that I have is a pretty legacy one. We do have servers, lots of servers."

Those servers bring a cumbersome amount of cost, operation and maintenance to the organization, the leader said, which has prompted the agency's team to look into the potential for cloud operations to alleviate that burden.

"My target is to get everything to the cloud," the leader said. "We want to take everything and push it out to the vendors who can manage it much better than we do. We are looking at the on-site services that we have and pushing them into cloud. It's a multi-step process."

And with that process comes a resistance to change, the leader said. Another leader, from a transportation agency, agreed and said that resistance makes it more difficult for government to keep up with more modern and efficient technology.

"I think there's a struggle there, and we've got a lot to learn," the official said. "We're pushing [our agency] to move from paper to electronic. You'd think everyone would be all excited about that, but they won't let go of paper."

That reluctance could come from a lack of understanding of what the technology-driven change could bring to the agency, the leader said.

"We're not all that comfortable with abandoning our traditional ways," the official said. "We just now created our first cloud data portal, and we're so excited, we're so proud. But the rest of the world's been doing it for a long time. I think we're behind the times, and could certainly benefit from where IT has advanced in other industries."

But modernization is not the only problem that legacy technology presents state and local government agencies. Legacy systems owned wholly by government agencies require regular upkeep and maintenance from government staff. While some of the upkeep and maintenance is efficiency related, a large portion of that effort includes patching and updating to protect against cybersecurity threats.

Cybersecurity

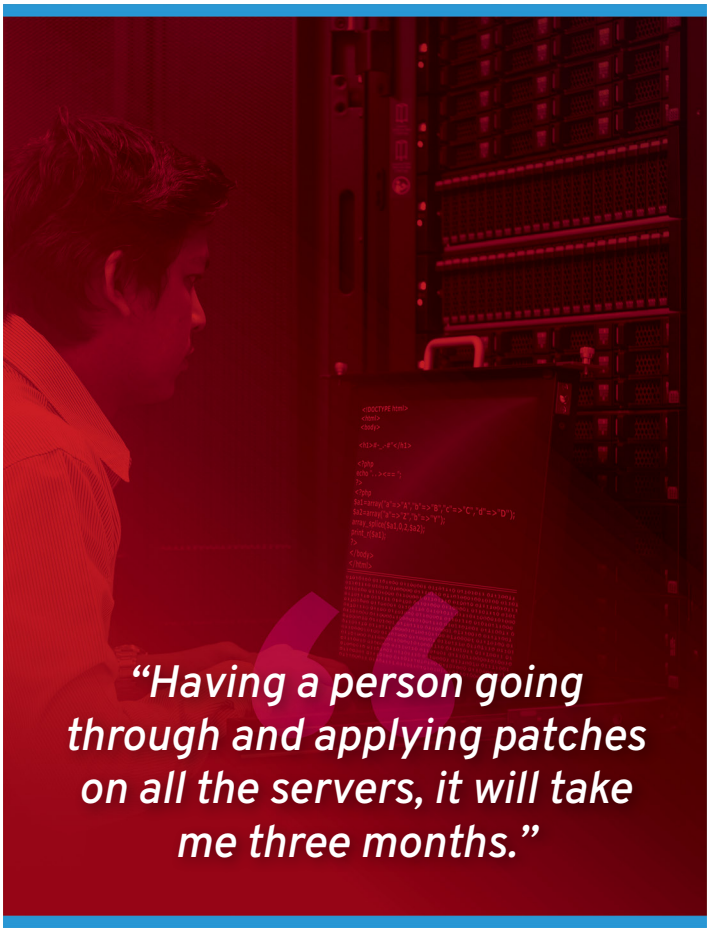
The updates and patches necessary to keep hardware like servers and machines secure can be a laborious task for agencies that maintain their own infrastructure. In addition, government staffs are almost always limited by budget constraints.

One agency CIO — who had only been in the role for a year — said at the roundtable that when they arrived, they were shocked to discover that the legacy systems present at the agency had not been updated in years.

"On the last virus outbreak, when I started to make inquiries, I find out that we hadn't patched our machines for years," the leader said.

That discovery prompted the leader to look at vendor-driven solutions that evaluate the infrastructure across the enterprise and automatically find and apply the patches and updates to ensure security.

"We ended up going to a cloud vendor who basically looks at everybody — including Red Hat — and downloads the patches and makes it ready for us, so it makes it somebody's job to just go in and say hit, go, and it doesn't matter what the machine is, either outside the network or inside the network, the machine will get patched."



Another technology agency leader agreed, and said that if their agency devoted staff just to those patches, it would be almost impossible to make a dent in the updates.

Agencies struggle with updates and patches now more than ever, one leader said. The topic is especially top of mind in the wake of high profile cybersecurity breaches like the compromise of up to 143 million Social Security numbers at Equifax. That breach was possible due to a cybersecurity vulnerability that could have been avoided with an update.

"I have hundreds of servers," the government leader said. "Having a person going through and applying patches on all the servers, it will take me three months. If there is a breach, I cannot go to my boss and say that I have been applying patches, but the patch came in 90 days back and I still have not applied it yet."

There simply is not enough manpower, the leader said. Government agencies do not have enough staff to keep up with patches and updates, especially with a years-long backlog of patches and updates to contend with.

Another leader said cybersecurity vulnerabilities cause agencies to be more reluctant to embrace emerging tech, which prohibits modernization and innovation across government agencies.

"As we begin to think about cybersecurity in this connected world, we're realizing that even our more traditional systems are not terribly secure," the leader said.

With connected devices — like traffic lights or sensors — as the pinnacle of the smart city movement, government is exposing themselves to additional risk, especially if those devices are placed on government networks and are unsecure.

"Anybody with the right key can do all kinds of things," the leader said. "That makes the network insecure, and there are all of these things that I want to do, but [cybersecurity officials] are not all that keen on that because I'm introducing additional IT security risk. I think there's a struggle there, and I think we've got a lot to learn."

Threading the needle with open source

With the challenges of legacy modernization and cybersecurity facing governments, technology officials need to find partners to combat the threats to their enterprise. Those partners, the government leaders said, come from other agencies within their own government, other levels of government, academia and the private sector.

"The old world of software is changing rapidly," one technology official said. "I think you're going to see more and more open opportunities, whether we call it open source, or open code, or whatever the new term is within the next three or four years, I think you're going to see a lot of movement in that direction."

The masses do more, the agency leader said. Government agencies are demanding more help addressing the challenges of cybersecurity, legacy modernization and other inhibitors to innovation. In response, the private sector will need to rise to the occasion and deliver results that work for the governments they serve.

"A lot of smart people out there see a lot of things that others don't," the official said. "When a lot of people are looking at the same picture, you can get resolution and advancements in a much more rapid manner that really helps."

And that's where commercially-supported open source comes in handy, one leader said. By having the code and information out in the open, researchers and members of the community at large — whether government, private sector or academic — can contribute, pitch in, and help increase efficiency and security along the way.

That efficiency and security makes the job of government delivery of digital services easier and cheaper, and can help narrow the gap between the present day and the adoption of emerging technology services.

"A lot of our equipment is 40 years old," one leader said. "But we have to take this opportunity to advance from a technical perspective and to try to do things to improve our customers experience and how they interact with us." What it really comes down to, one leader said, is finding ways to develop a structure and operation of an information technology agency "without boundaries." By modernizing their technologies with cloud and open source, agencies have a better chance to keep up with changes in service delivery, and increase the potential for growth.

"IT isn't just a support function anymore," a technology leader said. "The business demands operational efficiency, security and agility. Innovating the way you do that will drive business value and growth across the enterprise."

That innovation can come in multiple ways, the leader said, but it comes down to finding the right mix of established stable applications, as well as being agile enough to capitalize on new opportunities as technology changes.

"Both models of IT are required to be successful," the leader said. "Consistent, secure, open technologies support both the rock-solid conventional capabilities of IT and the fast-changing needs of agile IT."

This article was produced by Scoop News Group, for and sponsored by Red Hat and Intel, and distributed via StateScoop.com.

statescoop redhat intel