Cyber Resilience Around COVID-19 Latest IT Focus

Agency leadership is accelerating work on cloud adoption and remote information management to meet new challenges presented during the pandemic.

Adam Patterson
Mon, 05/18/2020 - 10:45

Federal leaders from the departments of Commerce and Homeland Security plus the U.S. Agency for International Development are detailing how they've implemented efforts that address security and information management after the agencies saw the impact that the mass move to telework across the country has had on operations.

Photo Credit: elenabs/iStock
"You’ve got to be able to do resiliency. Can the pipe handle it, can all these other aspects of working remote — phones, personal devices — be accommodated?" said Kevin Coyne, director of technology and services at the Department of Commerce, at an industry event May 14. "You’ve got to think of the whole gambit of IT services to make sure they’re supported."

This created a dual imperative to reconcile these changes with predetermined federal budgets while meeting projected IT developments and agency modernization projects.

“You may not have planned for this in your budget in your acquisition process, but you’ve got to respond to it,” Coyne said.

The COVID-19 pandemic appears to have widely encouraged an acceleration in the building of disaster preparedness and continuity of business processes across the federal government, particularly through a focus on enabling remote work on a larger scale.

“One of the things that will come out of all this is that agencies will get a better handle on continuity of government when everyone is forced to be somewhere else,” said Lon Gowen, chief technologist at USAID.

The abrupt transition to remote work has also served as an unintentional stress test that demonstrated the capacity — or lack thereof — for agency IT systems to support this level of satellite productivity.

“What we see here is a different scenario where we’re trying to keep up all operations [remotely]. It puts a pretty heavy load on the infrastructure of a country, state or municipality,” Gowen said.

This has led federal IT executives to quickly realize the importance of establishing and implementing a baseline of technical development that agencies will need to implement in order to support remote continuity of operations.
“We see great discrepancies between the IT maturity of different agencies,” said Norman Speicher, a program manager at the Department of Homeland Security Science and Technology Directorate. "What some of our projects are trying to do is level-set — provide a framework to build on, and we’re using a collaboration platform to set the lowest tier of entry, recognizing that if we create a secure and resilient environment there, we can eventually bring on other systems into that framework and build the consistency across agencies to be much more robust."

The challenges presented by remote work and data access appear to be accelerating federal agencies’ transitions to the public cloud, particularly through the merging of localized data centers with larger providers. This will be especially conducive for aiding data recovery and restoration of services amidst an emergency, a benefit that federal agencies had already been exploring.

“In my experience, agencies are evolving to embrace cloud computing. So they’ve got the unique situation of having historically owned their infrastructure ... and to embrace the new technology they’ve had to adopt a hybrid [cloud] solution,” Speicher said.

Beyond questions of meeting the demands of a remote workforce, agency leaders also seem attuned to the potential for malicious actors to exploit the uncertainty of the COVID-19 crisis to execute data theft. Speakers advised that team leads and IT executives remind their employees to be vigilant in upholding information security best practices.

“Any event like this provides an opportunity for attacks," Gowen said. "An easy one is obvious: let’s create an app that tracks COVID and make it a kind of Trojan Horse type thing. And so that’s the kind of stuff agencies are warning folks about. Be careful to use these kind of sites, go to trusted sites instead. People have a tendency to forget when one of these crises hits and they want to go out and grab the latest news."

Despite the challenges at hand, agency leaders expressed confidence in the technology solutions that could be adapted to federal agencies to ensure complete functionality during remote work.
“Can we go to a hyper-converged infrastructure solution that we can manage remotely anywhere versus physical servers you have to go touch?” Coyne said. "It’s really that acceleration of those technologies that are on the marketplace that most corporate entities have already moved to."

Beyond technical specifics, speakers also emphasized the importance of fostering internal coordination between IT experts and agency leadership to encourage the adoption of new technologies like cloud computing that will better enable remote work.

“You’ve got to know what the business needs are and get your team dialed in to deliver on that service so when they walk away there’s a deep appreciation for the IT team and they see the IT team as a partner,” Coyne said.