Education CIO Reflects on Security in Cloud Efforts

The agency is training its workforce and collaborating with partners to protect information.

Faith Ryan
Tue, 06/30/2020 - 09:53

The Department of Education has been relying on collaborative partnerships to effectively secure and consolidate its 100% cloud infrastructure, as well as workforce training to safeguard sensitive information from cyber threats.
Echoing other recent tech perspectives in government, CIO Jason Gray said the agency successfully pivoted to teleworking due to prior investments in IT modernization, particularly its cloud capabilities. It's also been mitigating new security challenges brought on by the new working environment through increased workforce education.

“The strategy that we've used has really been focused on educating the workforce because of some of the things that we've seen, [such as] waterhole-type attacks that are attempting to phish for credentials,” Gray said at a June 22 virtual event. “We've got great tools and applications that protect, detect and defend, but it's the human-error element we focused a lot on.”

The agency is also focused on close collaboration with others to mitigate cyber attacks. This includes federal agencies like the Department of Homeland Security and the Office of the Federal CIO, various vendors, and higher education institutions to effectively exchange information and leverage shared services.

“I found that's where we can really tap into the innovation because instead of spending our resources to try to create the wheel that's already been created, we want to leverage what has already been,” he explained.

Since the agency’s mission revolves around protecting student information throughout their educational careers, the need for data visibility through the cloud and updating legacy IT systems have also been critical to the department’s own technological development.

Over a year ago, the agency transitioned from an older IT services contract to a new cloud-service provider for cloud consolidation. “It was a heck of a journey so we don't have any on-premise [systems],” Gray said, “but I will say, the benefits were great.”

The move to the cloud paid off from both a reduction in cyber systems standpoint as well as administrative costs.

“We ended up going from $1.43 a gigabyte down to 12 cents a gigabyte, so [it was] massive in terms of the cost savings and in terms of the licenses that we were paying for,” he said.
The previous investment in cloud consolidation also made the agency’s shift to mass telework much more agile and flexible.

“[Over] a weekend, we transitioned over 400 terabytes of data from hundreds of servers and systems. From an on-prem standpoint, there is no way that would have been done in a weekend,” Gray said.

While communication and collaboration efforts remain strong for the agency, Gray said it is continuing to look for ways to partner with agencies and vendors for enhanced security, including robotic processing automation capabilities.

“From an RPA standpoint we have a lot of repetitive standard procedures that are done every single day by lots of people, and we're looking at ways to reduce that,” Gray said.

The agency is also looking to work with others on implementing a Zero-Trust framework and delivering other machine-learning capabilities, in which a device can automatically troubleshoot complex technical and security issues.

“We have a lot of data, and I want to be able to leverage that data so the department can proactively be making smarter decisions as it relates to risk and threats,” Gray explained, adding that collaborative efforts have been key to the agency's success so far.