Cloud Security Evolves

Agencies consider cybersecurity team members' roles and responsibilities.

Cloud has become a core part of the enterprise for many agencies. They have come to accept it can be as secure, or more secure, than their on-premises environments. However, as cloud becomes an integral part of an agency's enterprise, security becomes more important and agencies have to think about it differently.

This means better understanding cybersecurity roles and responsibilities within the cloud environment, improving training and awareness, and supporting government-wide programs designed to bolster cloud security, according to government and industry experts speaking at an Aug. 23rd Cloud Summit.

Cloud creates a new dynamic between agencies, users, and vendor partners with regards to their cybersecurity roles and responsibilities. Not only do those roles need to be clearly defined, but there also needs to be transparency in how they are carried out. Many agencies have made progress in this a rea, said Gregory L Garcia, Director, Corporate Information, Chief Information Officer/G-6, U.S Army Corps of Engineers. "It's not that cyber security wasn't there," he says. "I think it's the understanding of the roles and responsibilities that has matured."

The Corps plans to use the DISA cloud access point, and is still determining how best to define cybersecurity roles and responsibilities under this scenario, says Garcia. "I'm not sure we're done yet with understanding with how cyber will work—at least for the Department of Defense—in the cloud."

Information-sharing has to be a "two-way street" between the cloud service provider and the agency when mission critical applications are running in a commercial cloud, says John Hale, Chief, Cloud Portfolio Office, Defense Information Systems Agency. "That's the long pole in the tent. And it really has to do with in a war fighting situation, how do we continue to protect our applications when they're running in a commercial cloud providers' environment?"

Cloud security depends on a shared security model. "With cloud there are a lot of myths," says John Nemoto, Vice President, CGI. One myth that needs to be dispelled is the idea that when an agency moves an app to the cloud, it inherits all security and authorizations associated with the Federal Risk and Authorization Management Program (FedRAMP).

That is not the case, says Nemoto. Agencies must consider the application level, the system level, the network level, and the users involved in security. "Where [do] the boundaries of that security between the cloud service provider and your organization begin and end?"

FedRAMP is the federal cloud computing initiative designed to improve cloud security that has been helpful in speeding up cloud adoption in government. "Since FedRAMP launched we have doubled the number of cloud service providers and authorizations each year," says John Hamilton, FedRAMP Program Manager of Operations, U.S. General Services Administration.

The program has done this by providing a standardized risk-based approach to assessments, authorizations, and continuous monitoring. GSA has also been providing more training, guidance, training, guidance, and customer-focus customer-focused efforts to speed cloud adoption.

> "Where [do] the **boundaries of that security between** the cloud service provider and your organization begin and end?"
>
> **JOHN NEMOTO,**
> **VICE PRESIDENT, CGI**

DOD relies on FedRAMP to help it speed up acquisitions and help ensure cloud providers meet its cybersecurity cybersecurity requirements and controls, says Hale says. The goal is that as FedRAMP evolves to include more DOD security controls.

The Social Security Administration (SSA) relies on FedRAMP to provide a baseline for systems, whether it's Software-as-a-Service, Infrastructure-as-a-Service or Platform-as-a -Service, says John Morenz, Chief Technology Officer, Office of the Chief Technology Officer, SSA.

It's up to the agency to know what the shared controls are with its cloud service provider. "More importantly, you need to understand what is in FedRAMP and what is not in FedRAMP from these infrastructure service providers," says Morenz. "Not everything is under FedRAMP control."

As agencies push more information and infrastructure into the cloud, they should bring security and operations together to make it easier to manage and protect.