ATARC aws

Powered by GovExec

Building Secure Cloud Infrastructures: Insights from Federal Cyber Experts

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with AWS, November 2024

During a recent roundtable, Federal experts discussed various challenges with building and maturing secure cloud infrastructures amidst rapidly evolving technology. Discussion centered around cloud security and compliance, strategies for migrating legacy systems to the cloud, the concept of cyber resilience, and the impact of emerging technology on cloud infrastructure.

The Cloud Migration Journey

> **“We're redesigning our [cloud] journey. We’re on the cusp of a new age with AI. We’re just rethinking it all.”**

Panelists kicked off the discussion by emphasizing the importance of approaching cloud migration strategically and incrementally. Evaluating the entire business system holistically can ensure the right approach is taken with legacy systems that cannot be moved directly to the cloud without significant changes.

Many panelists are taking a hybrid approach to cloud infrastructure, operating both in the cloud and on prem. This is sometimes necessary because some legacy systems cannot be migrated to the cloud for practical, logistical, or security reasons. However, panelists also note that ‘lift and shift’ migrations are sometimes unavoidable.

Other agencies on the panel have implemented a shared services model. While there was some initial pushback, most services are now incorporated, particularly human resources and technical services. However, due to legislative requirements, some agencies must keep their functions separate, but those that have merged have experienced greater synergy.

Another agency has implemented an integrated product team (IPT) model, which brings together representatives from various departments to address technical problems and deliver solutions. Eventually, this group may evolve into a center of excellence and provide playbooks and guidance for on-ramping into the cloud environment.

Challenges with Cloud Migration

Panelists also discussed challenges with cloud migration, particularly with the complexities of data management and the bureaucracy of the ATO process.

Data Management

Agencies with large amounts of data sometimes struggle to locate and consolidate existing data spread across various systems to be used in cloud applications. To complicate things further, some of this data must remain siloed to ensure proper data security.

Panelists discussed the challenges of sensor integration and data management in the context of cloud infrastructure. With the influx of data from innumerable sensors and devices, agencies struggle to manage, process, secure, and effectively use the data. The influx of data from various sources into data lakes raises concerns among some panelists about security and the need for comprehensive, unified access to the data.

Panelists also noted the evolution of security and authentication of IoT devices, and emphasized the challenges agencies face with authenticating and securing these access points. Many sensors are segmented from the mainstream networks or legacy systems, and unfortunately have not yet been addressed.

ATO Process

According to some panelists, the ATO process creates a "chicken or the egg" scenario, where agencies need a cloud environment to obtain an ATO, but cannot establish the environment without the authorization. Additionally, the Authority to Connect (ATC) process adds another layer of complexity to fully take advantage of cloud capabilities. Overall, panelists believe policies surrounding ATO and ATC need to be streamlined so agencies can more easily follow the regulations, remain compliant, and continue making progress in cloud environments.

Staying Ahead of Emerging Trends and Technologies

Panelists continued the roundtable discussion by emphasizing the importance of proactive experimentation and strategic risk management to stay ahead of cybersecurity trends and anticipate future vulnerabilities.

> **"It's always a challenge to try to stay ahead of the curve when it comes to the adaptiveness of the cloud and the tools that we can use."**

- **Staying informed** - Panelists note that it's very important to stay plugged into emerging services, new capabilities, and other innovations in order to stay one step ahead of future vulnerabilities.

- **Conducting low-risk experimentation** - Panelists suggest evaluating the potential "blast radius" of a new service and the risk level of data being used. If risk can be lowered by controlling access points, then there may be an opportunity to accelerate adoption of new technology through low risk experimentation.

- **Ensuring data privacy** - Agencies are not only continuously securing data as it moves across the network, but are also being very intentional about building new cloud infrastructure to secure data.

- **Communicating openly** - Panelists emphasize the importance of building relationships and sharing knowledge with other organizations to stay ahead of the curve.

- **Implementing zero trust** - Panelists note that even with the best cybersecurity measures, a weak infrastructure can undermine the effectiveness of zero trust. As technology continues to accelerate, agencies must implement zero trust and utilize AI in cybersecurity.

Measuring Cyber Resilience

> **"Before you can measure cyber resilience, you have to define it."**

Panelists discussed the concept of cyber resilience, particularly with how to define it. Agencies measure cyber resilience differently, but there are tools available to help simulate outages and test the ability of infrastructure to self heal and react to vulnerabilities.

Panelists also discussed how cyber resilience is measured in various agencies, and some of the challenges in doing so. Several panelists note that cybersecurity priorities are often driven by top-down directives, rather than a proactive risk-based approach. These top-down priorities are typically reactionary and take priority over other actions that may build more cyber resilience.

Other panelists noted that cyber security is more of a challenge at the user level rather than in data centers. Agencies routinely conduct phishing campaigns, training exercises, and in-person events to educate users on cybersecurity best practices in order to build cyber resilience.

However, some panelists suggest operating just at the edge of compliance in order to make progress and achieve the mission. Some on the panel are implementing a new approach to cybersecurity by combining operations and security into one working unit to better respond to threats. Doing so forces the agency to consider how to further business objectives, maintain security, and bolster resilience.

Because cyber resilience is so widely defined, panelists underscore the need for well-scripted run books to help agencies troubleshoot and react to resilience issues. The goal is to have systems that can detect and automatically recover from outages, but identifying potential vulnerabilities in advance is also critical. Panelists recommend creating a framework to help agencies define different levels of resiliency based on access levels.

> **“Don’t let perfect security be the enemy of advancing innovation.”**

Panelists note that although agencies know how to achieve cyber resilience, there is little funding prioritized to achieve those initiatives. There are usually bigger issues that take priority, and talent turnover prevents agencies from building and leveraging an experienced workforce.

Making Change Happen

> **“Change is good, and change is always going to happen. So might as well embrace it.”**

Panelists then discussed challenges with effectuating short-term goals that feed into longer-term strategies. Generally, business owners often do not understand the severity of cyber issues within the agency, nor do they appreciate the value applications, software, and vendors have on the mission. Too often business owners are more preoccupied with cost rather than value.

Panelists also note that current policies are often written for legacy systems and do not adequately address the capabilities and requirements of cloud environments and emerging technology. In many instances, the way policies are written are preventing agencies from doing things the cloud is specifically built to do. Policies must be updated in order for agencies to effectuate upgrades and changes to cloud infrastructures.

Panelists suggest a need for more flexible guidelines, rather than strict policies, to enable agencies to more quickly adapt to new technologies. Similarly, some agencies are already shifting from an Authority to Operate (ATO) process to Authority to Use (ATU) to help streamline adoption of new technology.

LEARN MORE AT: HTTPS://AWS.AMAZON.COM/FEDERAL/