

How Agencies Can Build Their Data Resilience

Data has always been central to mission. With the rapid rise of artificial intelligence and the current drive toward improved efficiencies, agencies are under more pressure than ever to ensure the ready availability of data, even in the face of rising cybercrime, natural disasters and other perils.

At a recent [GovLoop event](#), experts from industry and government outlined strategies to strengthen data resilience. Here are insights from that discussion.

The speakers:

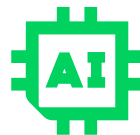
- **Vishal Chaudhry**, Chief Data Officer, Washington State Health Care Authority
- **Rick W. Vanover**, Veeam Product Strategy, Office of the CTO, Veeam Software



Go Beyond Compliance

Agencies face a range of security mandates that can help them improve data resilience, but those mandates, while necessary, are not sufficient in themselves. “Organizations have to really look at compliance as a starting point,” said Rick Vanover at Veeam Software.

Leaders need to frame resilience in terms of the mission itself, Vanover said: What data is mission-critical, and where does it reside? What are the intended use cases? “Organizations have to really double down on the stacks that matter, supporting them with the highest level of operational excellence you can,” he said.



Keep Up With the Technology

In the realm of backup and recovery — the core of data resilience — tools powered by AI are driving rapid improvements. Agencies should take a thoughtful approach as they explore the many solutions now being branded as AI-enabled, said Vishal Chaudhry at Washington State Health Care Authority.

“AI is not one monolithic, homogenous thing. There are a variety of different techniques and approaches that can be used to augment and support what we need to do,” he said. Which tool will best serve the mission needs? “We just need to be thoughtful about it,” he said.



Align Tech to Business Need

As agencies look to bring new tools to the fight, they must align their resilience strategy to the needs of the mission. “Understanding the risk profile of the different parts of the business is absolutely critical,” Chaudhry said. For each data-driven business process, leaders should ask things like: What is the impact of a failure here? What is the risk if this part of the system goes awry? “Those are important conversations that need to happen before you implement a system,” he said.

Aligning to mission will mean, among other things, deploying AI-informed solutions that protect against human error. “When I do make a mistake, does a system have functionality built in that alerts me to that? ‘Hey, you did something that you probably weren’t supposed to do. You want to double-check,’” he said.

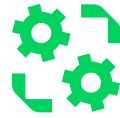


Take a Fresh Look at Backup

With capabilities that include instant recovery, automated recovery verification and immutable storage, “the backup offerings of today are far more innovative” compared with just a few years ago, Vanover said.

IT leaders will want to explore the latest options to ensure data is protected and can be readily restored in the event of system failure or ransomware exploit. Immutable storage, which prevents data from being altered or deleted once it’s written, is especially important when it comes to ransomware recovery, he said.

➔ To learn more, watch the full session [on demand](#).



Focus on Continuous Improvement

Resilience is not a one-and-done effort. Instead, it will be important for agencies to commit to continuous improvement and assessment, checking and rechecking systems to ensure they can support a rapid return to full operations in the event of a disruption, Vanover said.

That includes tracking new and emerging threat behaviors to ensure their responses align with the risk. IT team members who aren’t directly engaged in cybersecurity must nonetheless envision themselves as supporting the ongoing cyber response strategy and work accordingly. “I’m not saying spend 24 hours of every day working on that only,” he said. “But at an absolute minimum, quarterly reassessments and keeping systems up to date goes a very long way.”



Motivate the End Users

In the era of ransomware, end users are integral to resilience. Often, it’s their behavior that will trigger a breach and necessitate data restoration efforts. Agencies need to help front-line users of technology “understand and appreciate the sensitivity, the nuances and the importance of protecting the data,” Chaudhry said.

That training tends to stick when it’s tied to the mission and goals — the reasons why people got into government work in the first place, he said. “We don’t work for state government in the health care authority just because we need the job. Everyone of us works here because we are proud to be public servants and want to serve the people,” he said. “Bringing that to bear, making sure that is crystal clear — that helps a lot.”