PRESIDIO FEDERAL

Silver Business Partner IBM

As Agencies Usher in Hybrid Work, They'll Need New IT to Support It

As agencies embrace a mix of remote and in-person work, they must also adopt new strategies and technologies to ensure productivity, collaboration and connection.

OVER THE LAST SEVERAL YEARS, there has been much speculation about what the future of government work will look like. Will all employees return to the office? Will remote work be the order of the day? The answer, it seems, is shaking out somewhere in between: Hybrid work, a term that means a workplace allows someone to split their work between home and the office, is proving a popular choice. In fact, according to the Remote Employee Experience Index, 72% of employees surveyed noted that they preferred a hybrid remote-office work model.

This preference is likely because a hybrid work environment offers employees the ability to work in whichever environment they find the most productive — a preference that can shift daily depending on tasks being performed and family needs.

"I think we're thinking of those days where you can be very productive working at home. And then those days where you want to be with your colleagues or clients collaborating and innovating," said Joanne Wright, vice president for enterprise operations and services at IBM during a recent interview about IBM's own move to hybrid work.

As agencies seek to embrace hybrid work environments, however, they'll need not just new policies, but technology that can improve connection and collaboration for employees from any location. This includes technologies like hybrid cloud and security tools that can keep constituent and government data safe in a rapidly evolving cyber landscape.

Rethinking Your Cloud Strategy to Support Hybrid Work

When the pandemic started, many agencies quickly moved to adopt cloud to enable remote and digital operations. Now, however, agencies should use the return to work as an opportunity to evaluate whether their cloud infrastructures

are adaptive enough to support the needs of a hybrid workforce.

For example, as employees enjoy more flexibility in the workplace, IT environments will need to adapt to introduce a greater degree of flexibility, as well. And it's not just employees that have their eye on flexibility; a 2020 IBM CEO study notes that 56% of the CEOs surveyed said enhanced operational agility and flexibility is their top priority in the next two to three years. And according to another recent study from IBM, by adopting hybrid cloud, agencies can more quickly transform IT operations to better support agility and collaboration. Moreover, it can equip an organization with the foundation it needs to pivot quickly to address new challenges or changes, provide employees with access to the data and applications they need no matter the geographic location, as well as provide employees with the tools necessary to innovate quickly and effectively.

"Open hybrid multicloud offers the flexibility necessary for business innovation and improved customer experience, while also addressing security and cost concerns," according to IBM's "Government On Open Hybrid Multicloud" report. "It can serve as the necessary foundation for a modern government architecture by enabling internal and external data accessibility, workload flexible portability, and effective interoperability of analytics."

Prioritizing Cybersecurity

As public sector employees moved quickly to remote work in early 2020, malicious actors took advantage of the shift and cyberattacks such as phishing and ransomware soared. Now, as the U.S. finds itself in a particularly tenuous cyber environment, agencies need to ensure that the shift

to hybrid work doesn't inspire similar action — and that security concerns don't hold them back from adopting tools, like cloud, that can help improve workflows and help agencies meet the mission.

However according to "Government Index for IT Modernization", a new study of current and former U.S. government IT decision makers, commissioned by IBM, nearly 70% of those surveyed view security risks as the top barrier when migrating to modern cloud platforms, holding many agencies back.

To effectively protect government workers and data in this new environment while embracing modernization, agencies can take a few steps to help shore up cloud security, including:

- Considering open and secure hybrid cloud architectures to embrace innovation in the cloud which focus on helping them keep their data protected. "A hybrid cloud approach can help governments manage data across on premise, off premise/cloud and edge environments, securely," IBM noted in a recent press release.
- Reduce complexity and help to mitigate third party risks by encrypting data and implementing confidential computing to protect data in use.
- Adopt new approaches to cybersecurity, such as a zero-trust architecture, to help protect data across hybrid cloud environments – no matter where that data resides.

Building a Hybrid Work Strategy

There's no doubt that the workplace of today looks vastly different than it did just a few years ago. And if there's one thing agencies have learned about how employees work most productively, it's that there's no single option that fits every employee. Similarly, there's no one-size-fits-all option for a productive and secure hybrid remote environment.

As government agencies look to make space for each employees preferred way of working, the best way to ensure employees remain productive, innovative, and secure in a hybrid work environment is to plan ahead. As agencies begin to strategize what their hybrid work environments will look like and how they will best serve public servants, experts and tools from IBM, like IBM Watson Works, can help agencies plan effectively for a productive, secure and innovative workplace.

For more information about how IBM and Presidio Federal can help your agency adapt to the ever-changing times, please visit:

Hybrid Cloud and AI Are Driving the Future of Work: Are You Ready?