IBM Newsroom

IBM Survey: Government IT Modernization Driven by Security Concerns

Escalating Cybersecurity and Ransomware Attacks Make Spend on Cybersecurity a Priority for Government Agencies Next Year, Many Agencies Expect 3 Plus Year Timeline to Comply with New Cybersecurity Executive Order

ARMONK, N.Y., July 15, 2021 /PRNewswire/ -- According to "Government Index for IT Modernization", a new study of current and former U.S. government IT decision makers, commissioned by IBM (NYSE: IBM), nearly 70% of those surveyed view security risks as the top barrier when migrating to modern cloud platforms. Of those surveyed, security also now outweighs reducing costs by almost double as the reason to modernize IT infrastructures.

Recent cybersecurity threats including SolarWinds, one of the largest supply chain attacks in recent history, and the Kaseya cyberattack impacting 1,500 global organizations, have put a spotlight on current cyber threats and existing vulnerabilities. In an urgent response, President Biden issued an executive order, urging federal agencies to modernize and protect their data from existing and future threats.

As federal government agencies look to make decisions for their long-term strategies, IBM's new market research, "Government Index for IT Modernization" provides insights into the critical role of security and privacy in cloud adoption and modernization decision-making. The study, conducted by Morning Consult on behalf of IBM, surveyed over 500 current and former IT government decision makers based in the U.S. found:

- **Modernization Drives Security** - With cybersecurity attacks on the rise, so too are budgets to protect data. Responding government IT decision makers for all levels of government anticipate agencies will spend the most on cybersecurity in planning for FY22. According to the study, more than 75% of respondents cited migrating and managing data from legacy systems to the cloud as a challenge for their current or former agency, with security was cited as the top barrier but also as a main driver.

- **Contradictions Over Security Readiness** – The study found that between 64% and 82% of respondents believe their current or former agency is very prepared or somewhat prepared for a wide range of current and future threats - from ransomware to post-quantum attacks. Yet more than 40% believe it will take three or more years to comply with the Biden Administration Cybersecurity Executive Order to implement zero trust and encrypt all data, an eternity in a world where security breaches occur with increasing regularity. This contradiction is further reinforced when looking at the current use of baseline security protocols – more than half of IT decisions makers surveyed say their cloud administrators does not always require complex passwords (50%) and two-factor/multi-factor authentication (51%).

- **Visibility Gets Cloudy** - 50% of the respondents report their agency is using a mix of security tools for on-premise and cloud threats, creating a gap in visibility. At the same time security is the top concern holding 46% of responding government IT decision makers back from working with third party vendors. With the average federal agency using 10 or more cloud providers and working with hundreds of third parties, managing risk across this growing attack surface is expected to further complicate security.

"With the President's executive orders, the U.S. Federal market is facing a massive transformation to its cybersecurity strategy which requires a great deal of technological modernization. While this is a priority for government IT decisions makers, our survey found that they view security as both a driver and barrier to modernization," said Howard Boville, Head of IBM Cloud Platform. "Enterprise technology providers are stewards of massive volumes of personal data, and we need to do our utmost to

protect this data. A public and private sector partnership that adopts an open and secured hybrid cloud architecture with sophisticated security capabilities can help agencies ensure that data truly remains theirs, even in a multi-cloud environment."

Managing Transformation and Risk in Hybrid, Multi-Cloud Environment

IBM has a long history of collaboration with the U.S. Federal Government helping it innovate, adapt and transform over a multi-decade journey. This includes helping government agencies ease cloud adoption, improve efficiency, bridge varied cloud environments, and ensure mission critical workloads are integrated with security.

Based on the results of the new study, IBM suggests the following insights for managing risk while modernizing:

- Government entities should consider 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.

- Complexity is the enemy of security and the approach to modernization should incorporate a secure architecture, including sophisticated capabilities that will not compromise or monetize customer and citizen data at any cost. To help mitigate third party risks it's vital to close any loopholes in the data security supply chain, encrypting data being stored and transmitted and leveraging confidential computing to protect data in use.

- New approaches for cybersecurity should be adopted to help protect data across hybrid cloud environments – no matter where data resides – either on premise, in the cloud or at the edge.

For more information about IBM's work in the US Federal market, visit: https://www.ibm.com/industries/federal

Methodology
The data sheds new light on how government decision makers view obstacles to IT modernization. The research is based on more than 500 responses collected among current or former government IT decision makers in the United States across local, state and Federal government entities. The polling was conducted online through Morning Consult's proprietary network of online providers in June 2021. All respondents were required to have significant insight or input into their agency's IT decision-making.

Contact:
Kaveri Camire
IBM Communications
kcamire@us.ibm.com
Suzanne Cross
IBM Communications
Suzanne.cross@us.ibm.com

SOURCE IBM

Additional assets available online: Photos

https://stage.mediaroom.com/ibmnewsroom/2021-07-15-IBM-Survey-Government-IT-Modernization-Driven-by-Security-Concerns