Adopting zero trust data security in the cloud

Protecting data from intrusions and recovering quickly from an attack are hallmarks of a modern security plan

Jared Vichengrad

Rubrik

Before the pandemic, government agencies had a business model that required employees to be in the office and required constituents to seek services in-person. When government facilities closed to both employees and the public in response to the pandemic, agencies were forced to rethink their operations. Many employees are still working remotely at least some of the time, and many Americans are demanding even more digital services.

The solution to both challenges is to modernize the IT infrastructure to remove the obstacles that lock agencies into a physical versus virtual experience. Even more so these days, we are seeing the consolidation of data centers and the move toward cloud-based technology. That switch allows the government to be more nimble and ultimately provide a better digital experience to its customers.

Agencies are aware of most of the risks involved in moving to the cloud, but unfortunately, many security plans overlook the need to protect all the data the government collects. As long as those plans focus on networks and endpoint devices without a corresponding focus on securing data, agencies will continue to be vulnerable.

Minimizing risks and maximizing recovery

It's not a matter of if an attack will happen, but when. Research suggests that cyberattacks will continue to intensify, and although ransomware has been a global threat for some time, it has recently increased so much that it is a household word. Ransomware is something that every person in an organization must focus on avoiding by recognizing suspicious email messages, not opening them and certainly not forwarding them.

Hackers are now multibillion-dollar organizations, and they have always targeted government agencies because of their legacy data backup and recovery systems. Therefore, agencies should develop data protection plans that involve modernizing backup and recovery solutions so they can quickly respond to an attack and regain access to their data.

Rubrik offers zero trust data security so that agencies can gain maximum protection against hackers. We focus on reducing intrusion risks, monitoring sensitive data and enabling agencies to rapidly recover from an attack. Above all, we want agencies to avoid the need to pay any ransom.

Cybersecurity and the citizen experience

On the National Association of State CIOs' 2022 list of its members' top priorities, cybersecurity is in the first slot, followed by citizen experience. Those two go hand in hand. When a school is hacked and its data stolen, that school will likely be forced to close for days. When a department of corrections is hit with a ransomware attack, it will be in lockdown. And when

Nick Iliasov

> ## "Hackers are now multibillion-dollar organizations, and they have always targeted government agencies because of their legacy data backup and recovery systems."

a public health department's systems are breached, it will be unable to provide vital services.

Those are real-world examples of impacts that are happening across the country, and they illustrate why government agencies can't wait until tomorrow to address these vulnerabilities. CIOs, chief security officers and IT directors at all levels of government know they need to do something today because they are vulnerable every minute until they do.

At Rubrik, we focus on simplifying the protection of data in the cloud while keeping the citizen experience up and running. We are proud and excited that Microsoft has invested in Rubrik to develop and deliver integrated zero trust data protection solutions built on Microsoft Azure. That partnership demonstrates both our companies' commitment to protecting government data and making the cloud a more secure and productive space for citizen services. ■

Jared Vichengrad is vice president and head of state, local government and education at Rubrik.