What the COVID-19 Pandemic Has Taught Us About Preparing for the Next Disaster?

Joseph Klimavicz
Deputy Assistant Attorney General
Chief Information Officer and Chief Data Officer, (retired)
Department of Justice
Managing Director, KPMG LLP

Today, digital technology is ubiquitous, digital collaboration is woven into everyday life, and artificial intelligence is available at our fingertips, fueled by the availability of staggering volumes of data generated from the billions of interconnected devices. During the COVID-19 pandemic, the federal government has taken the largest workforce in the country and moved them to remote environments, while continuing to provide the most important services to the public. However the pandemic has highlighted five (5) strategic imperatives to prepare for the next disaster. We don't know when the next disaster will occur or what it will look like, but we do know we can develop mitigation strategies.

The first imperative is to **embrace remote access as a permanent capability**. Remote or virtual workers have never been a core framework of government's workforce strategy. Stay-at-home orders sent government workers home almost overnight, and while it has been difficult for many, the bottom line is that the government workforce is productive working remotely. We now have an agile workforce not tethered to a specific location delivering services. This in turn has created the opportunity to embrace a virtual workforce as part of an operational strategy rather than a temporary measure.

The second imperative is to **move critical services to the cloud**, including those previously reserved for on-premise, and build in resiliency. A single cloud maybe robust and secure, but it still represents a single point of failure, and a multi-cloud environment enables agility, flexibility, and resiliency at a lower cost. It allows tailoring to fit varied needs within the organization, and has the elastic capacity, on-demand provisioning to bring together data and analytics with sufficient compute.

> "Stop developing scenario-based COOP plans that lead to a false sense of preparedness and readiness, and do not provide the flexibility to pivot to the next event or circumstance."

The third imperative is **leverage data as a strategic asset**. Remote workers expect their data to be online readily accessible when they need it. Everyone is using VPNs to access the data and so the physical location of your data is less important than how you manage your data. This means building enterprise capabilities, starting with a data strategy and a data architecture to optimize the value of data across the enterprise. You will also need a data investment plan to document specific actions to close data maturity gaps. These plans should address managing data across a multi-cloud environment, to include data virtualization.

The fourth imperative is to **protect the enterprise while maintaining agility**. Given your workforce, technology and data are all remote, the time has come to evolve from a static perimeter defense that does not al-

Continued on page 28

Joseph Klimavicz is a Managing Director with KPMG LLP where he leads the government Chief Information Officer (CIO) advisory practice and helps government clients develop and implement digital transformations. Mr. Klimavicz's 37-year career in the federal government began with the Central Intelligence Agency (CIA) as a scientist and culminated with the U.S. Department of Justice (DOJ) as Deputy Assistant Attorney General and CIO from May 2014 until March 2020. Mr. Klimavicz also served as National Oceanic and Atmospheric Administration (NOAA) CIO and Director, High Performance Computing and Communications from 2007 until 2014, and as the National Geospatial-Intelligence Agency Deputy CIO from 2003 to 2007. In 2012, Mr. Klimavicz received the U.S. Presidential Rank Award for Distinguished Executive Service, and he is a CIO-SAGE at the Partnership for Public Service.

low you to take advantage of cloud agility and move toward a zero-trust architecture. Zero-trust is based on the premise that cyber threats can originate anywhere, and we cannot trust the user's identity, the device, the workload, the network, or the data. With zero-trust, we redefine access with a software-defined perimeter that segregates users, devices, data, networks and services, and the architecture is designed so each entity is granted the minimum resources to perform its function.

The fifth imperative is **stop developing scenario-based COOP plans that lead to a false sense of preparedness and readiness, and do not provide the flexibility to pivot to the next event or circumstance**. We annually reviewed and revised COOP plans, but it was viewed as just another compliance exercise. And when the time came for the annual test, it was typically deferred to a later date. We must transform fragmented business continuity capabilities into a unified, enterprise-level crises response.

We are going to see a continuing demand from the public to make it easier to conduct business with the government from home, and the government workforce will continue to ask for workplace flexibilities. This will require continued digital transformations and will present a great opportunity to implement these imperatives. ■