COVID-19 brought to the forefront the realization that many Continuity of Operations (COOP) plans were either outdated or insufficient for the moment. Often created as a compliance necessity, many COOPs were static and built around anticipated scenarios or outdated frameworks. Cyber security operations have been part of this process, supported by rigid plans that have not reflected the dynamic environment of today’s cyber landscape.

Current state

For many reasons, government entities have fallen behind in modernizing their COOP plans for business and technology resilience and agility. Documents can be unnecessarily lengthy with plans and testing exercises that are scenario-based and focused on the failure of specific systems or impacts to single business processes. Cyber security operations are often segregated, rather than integrated into the plan’s testing and recovery. And for the most part, all plans are reliant on a workforce located close to the operations hub.

There is a lack of understanding about what COOP is and what personnel need to do in the event of a COOP declaration. The script is not clear and is not sufficiently practiced. Emergency management and COOP are often conflated internal to the organization. Core components of resilient organizations, such as continuity preparedness, response, devolution and pandemic operations, and recovery (reconstitution), are not routinely part of planning or well communicated.

What needs to change?

For government entities to mature their resilience and strengthen their agility, they need to:

— Embrace remote access as a permanent capability
— Move security operations and infrastructure to the cloud
— Stop developing COOP plans that are scenario-based and build agility into every plan from the start.
Remote access as a resiliency and agility strategy

Remote/virtual workers have not been components of government’s workforce strategy. Typically, government workers are located in geographic clusters such as Washington D.C., state capitals or county seats. As technology shifted and transformed, it could be argued that one of the reasons for the dominance of on-premise infrastructure and applications was that the workforce was there too, delaying the urgency to shift and realize the benefits of migrating to the cloud. From a budgetary perspective, desktop computers can be less expensive than laptops, further anchoring the worker to the physical location. And still—even in the year 2020—internet and broadband connectivity can be challenging in some locations. And then came COVID-19.

The need to quickly shift most or all government workers to remote access has exposed weaknesses, highlighted untapped benefits, and opened new opportunities for resiliency and agility. Government organizations, by and large, lacked sufficient policies, procedures and technology to support en masse remote work. And the workforce often lacked workspace at home to accommodate full-time remote work. Together, however, they have made it work by removing barriers, making infrastructure improvements, and shifting the workforce model. What is in place now is an agile workforce that should be viewed as part of a longer-term strategy for organizational resiliency and readiness. While not every government function can be fully online, we’ve learned from the public their willingness to embrace the transformation to more online services and the need for fewer face-to-face services. Government organizations should embrace remote access as part of their operational and COOP strategy rather than it being a temporary reaction. In addition to the resiliency and agility components, there are numerous benefits to the workforce. The remote access strategy can be beneficial to recruitment and retention, especially in the cyber security field, where there are more open positions than qualified and trained staff to fill them.

Move cyber security to the cloud

To achieve cyber security agility and the needed continuity of operations for any situation, cyber security infrastructure, tools, and data need to move to the cloud. The cloud, with its ubiquitous nature, provides unparalleled access to cyber data for your remote workforce. Locating your cyber data in the cloud means it will always be available to your workforce, and through data virtualization, you will not need to download or even move the data between clouds in order to operate on the data. Cyber security organizations need to evolve their capabilities to enable a cloud transformation of the business and benefits realization. Development of a risk and value-driven cloud security model is a foundational step in cloud transformation and should provide critical considerations for the initiation of this journey. With an ever-growing remote workforce as the new normal, identity and access management risks are more critical to mitigate, and all the data needs to be encrypted at rest, in transit, and during any analytical processing.

In addition, government agencies need platforms capable of processing very large cyber data sets at near real-time velocity. Artificial intelligence and machine learning (AI/ML) are embedded in most threat-based security analytics products now, and the result is that tremendous amounts of data are produced, collected, and analyzed on a continuous basis. The elastic capability that brings together cyber data with sufficient compute capabilities to effectively combat the evolving cyber threats only exists in a cloud environment. A commercial cloud environment provides highly elastic and scalable data storage, compute and analytics capabilities—all critical to modern cyber security operations. Clouds are built with immutable infrastructure and highly available, fault-tolerant architectures, capable of delivering on-demand provisioning.

As we move to the cloud, as well as tackle legacy threat vectors, the time has come to evolve from a static perimeter defense and move toward a zero trust architecture to help address complex cyber challenges that can originate anywhere. These cyber challenges are exacerbated by a distributed workforce, move to the cloud, remote work considerations and a proliferation of devices. Implementing zero trust needs to include: strong identity management, modern and capable software defined networks, and advanced analytics in order to protect assets, data and services. Zero trust needs to effectively mitigate third-party full supply chain risks for products, services, or companies. And although not directly related to zero trust, your cyber security architecture needs to include implementation of micro-virtualization (application-level isolation from the OS), micro-segmentation (dividing the network and reducing the number of users per network segment), and continuous access monitoring and data encryption.
Government organizations need to stop developing scenario-based COOP plans and instead take an effects-based approach to consider risks and impacts of negatively impactful events. Further, they should Test, Train, Exercise and Evaluate (TTE&E) organizational performance of plans and procedures on an ongoing basis to help ensure an ongoing state of readiness to address a COOP-level event. Scenarios limit organizational agility and do not provide the necessary flexibility to pivot based on the event or circumstance and cannot address the greater operational complexity that exists. There is often a lack of clear orchestration of COOP activities across agencies where departments do not understand business process connection points and interdependencies with each other, including the supporting IT infrastructure, systems, and applications. And many organizations today do not have a clear playbook that clearly defines and articulates who is to do what in the event of a COOP declaration.

The role of continuity governance as a compliance task must rapidly transform to that of an integrated and broader set of government requirements and standards. Government must transform fragmented business continuity capabilities into a unified, enterprise-level incident and crisis response that is guided by federal, state, and industry standards implemented throughout the organization. There is a need to reevaluate and reinvigorate continuity efforts so that organizations build it as part of its core business processes, with risk-based consideration given to business and mission impact as an ongoing part of organizational investments and initiatives.

KPMG can assist government entities in maturing their resilience and strengthening their cyber security agility. Our team members have substantial experience applying federal continuity regulations and directives as well as leading commercial industry standards. The cloud is enabling entirely new ways of doing business with agility to scale at business speed. That makes setting a clear cloud strategy, to include cyber security, and preparing for change, crucial to achieving business imperatives. We help clients determine where, when, and how to effectively use cloud technology and services. Our cloud strategy approach leverages leading insights, fostering collaboration between the business, IT, and cyber teams—ultimately delivering a cohesive strategy to build agility and resilience into your cyber security operations.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Contact us

Tony Hubbard
Principal
Government Cyber Security Leader
E: thubbard@kpmg.com

Joseph Klimavicz
Managing Director
Federal Technology Enablement Practice
E: jklimavicz@kpmg.com

Kathy Cruz
Director
State and Local Technology Enablement Practice
E: kathycruz@kpmg.com