MIT Executive Study Uncovers Top Government IT and Pandemic Resilience Trends

How Covid-19 Changed Government Organizations’ Priorities
Strategic Insights from Government Organizations

As governments worldwide mandated COVID-19 shutdowns, few government organizations expected what occurred shortly thereafter—sudden, dramatic proof of the value of digital technologies. Now as governments strive to make their IT organizations resilient, new enterprise technology priorities are emerging. It turns out that federal, national, state and local organizations that are “future ready”—possessing technologies that are highly flexible and capable of fully supporting work anywhere—are best positioned to succeed in the uncertain times ahead.

Here are the top 8 takeaways from a survey and series of in-depth interviews with 100 government executives as part of 600 respondents about the pandemic’s effect on IT conducted in June 2020 by the MIT Technology Review in partnership with VMware.

*In this survey, digital transformation is defined as “the incorporation of modern technologies into an organization’s processes and strategies to achieve business goals, such as improving customer outcomes or operational agility.” Examples include migrating applications to the cloud and automating company operations.*
Strategic Insight #1

The Pandemic Has Accelerated Government Digital Transformation—Busting Out Of Slow, Steady Norms

70% of government respondents believe their digital transformation efforts have been accelerated by the pandemic.

Seven in ten MIT Technology Review government survey respondents (70%) believe their digital transformation efforts have been accelerated by the pandemic. COVID-19, it appears, is a catalyst for speeding implementation plans for next-generation technologies across agencies, busting out of slow and steady progress norms. Across industries, healthcare respondents (89%) were the most likely to cite accelerating digital transformation due to the pandemic, which industry leaders believed also is removing decades-long barriers.

Takeaway: Government IT organizations are respond faster with digital technologies becoming the only ways to transact business and engage with constituents and other departments.
The goal is to become future ready. Organizations that achieve this status possess digital foundations supporting any cloud, any app, and any device so they can better respond to change—ensuring continuity as well as resiliency. Of the 30% of government organizations that have not accelerated digital transformation, there are two possibilities. Either they were already moving fast to seize digital-first initiatives that no acceleration was necessary, or their technology infrastructures were so antiquated they were hard-pressed to know where to begin. The former government organizations are well on their way to resiliency.

Strategic Insight #2

New Digital Services Add to Existing Cyber Security Challenges

51% of government leaders are allocating a significant share of their IT budget to security and threat management.

Government agencies continue to introduce new digital services. The number one priority and challenge is protecting against cyberattacks and securing data and information according to government leaders surveyed. As federal,
national, state, and local organizations adjust to new risk realities, close to half of respondents (51%) indicate they are allocating a “significant” share (defined as more than 25%) of their IT budgets to security and threat management. And almost half of government respondents (47%) indicate they will put more emphasis on defending against cyberattacks over the next 12 to 18 months—particularly endpoint risks.

**Takeaway:** Global organizations saw a 148% spike in ransomware attacks early in the pandemic. Future ready organizations recognize that distributed workforces widen potential attack surfaces and have moved to strengthen their security postures with zero-trust, least-privilege policies and controls across on-premises, cloud, and endpoint devices.

They leverage intrinsic security to automatically embed protection everywhere. This is a fundamentally different approach from “bolting on” security products. By deploying intrinsic security, government organizations looking to fortify operations can pivot to a strategy that leverages infrastructure and control points in new ways across any app, any cloud, and any device. When combined with threat intelligence, government security teams can shift from simply reacting to proactively protecting their environments from positions of strength.
Strategic Insight #3

Expanded Public Cloud Activities Invite New Challenges

#1 app challenge for government is maintaining governance and compliance.

Government IT leaders report that their organizations’ adoption of cloud—to infrastructure-as-a-service or platform-as-a-service (IaaS and PaaS) environments as well as user-facing software-as-a-service (SaaS) applications—accelerated during the crisis, and is expected to continue to rise. Public cloud workloads are growing, albeit slowly, due to COVID-19, the survey shows.

On average, 10% of government applications were hosted in the public cloud prior to COVID-19. This number is expected to increase to 19% over the next 18 months. Yet cloud adoption during the crisis has introduced challenges, especially with regard to compliance. A majority of government decision makers (68%) cite “maintaining governance and compliance regulations, for example, patching apps to meet security/compliance requirements” as a
top application challenge because of their expanded public cloud activities.

**Takeaway:** An increasing abundance of FedRamp Authorized cloud services are now available to power enterprise infrastructure and apps. This gives government organizations the flexibility to rapidly meet new demands.

For example, organizations seeking to modernize apps can leverage commodity SaaS productivity apps while focusing on refactoring and replatforming their mission-critical applications. And by adopting a unified digital foundation, government organizations can simplify public and FedRamp authorized cloud adoption and seamlessly extend to multi-cloud without having to reskill or retool.
Strategic Insight #4

Citizen Engagement Rises in Priority, And Is Becoming Cloud-Powered

67% of government IT leaders indicate that they have expanded their Agile practices and continuous delivery (CD) methods due to COVID-19.

The MIT Technology Review survey reveals that government cloud adoption and application modernization are happening simultaneously. A third (34%) of government organizations surveyed are increasing constituent digital experience priorities to better address constituent needs as a result of the pandemic. An obvious change has been greater online accessibility to public services and pandemic loan applications. One of the first signs of changing priorities resulting from the crisis is that nearly four in ten government respondents (36%) accelerated adoption of a cloud-based platform that supports modern application development. Moreover, an impressive majority (67%) of government IT
leaders indicate that they have expanded their Agile practices and continuous delivery (CD) methods in response to demands resulting from COVID-19. About than a third (31%) have instituted “secure-by-design” application development.

Government is not alone in prioritizing digital experience. With apps facilitating contactless payments and a host of other services, 98% of financial services leaders surveyed say they are increasing or maintaining focus on customer needs in digital-first customer experiences within apps—because of COVID-19. And more than half (51%) of healthcare organizations surveyed are increasing patient experience investments. The most obvious has been the ballooning of telehealth services worldwide.

**Takeaway:** Improving the application portfolio is key to improving the customer experience, according to a recent *Forrester survey*. Legacy application development and delivery models across government are costly and ill-equipped to support cloud-native and other modern apps.

Applying Agile practices and continuous integration/continuous delivery (CI/CD) models help organizations easily support changing requirements, especially when modernizing apps to enhance the citizen experience. And as outside events continue to drive digital transformation, flexible, automated technology environments allow for more fully digital experiences and greater agility.
Strategic Insight #5

Resilient Infrastructure Is Key to Efficiency

Top infrastructure initiatives increasing in priority due to COVID-19:

- **36%** Adopt a platform that supports modern app development
- **36%** Leverage infrastructure to provide security for apps and data regardless of where they reside
- **31%** Expedite cloud services adoption to meet capacity and scale demand

Telework numbers skyrocketed during the crisis (see takeaway #6), and governments expect those numbers to remain elevated even after the pandemic passes. This shows long-held leadership attitudes are shifting while raising questions about how to sustain hands-on IT operations across a widely distributed organization. When questioned about resilience, 56% of government organizations surveyed prioritized infrastructure efficiency as key to success, adding a significant share of their IT budgets to infrastructure efficiency. And the infrastructure efficiency initiatives they plan to accelerate next are adopting modern development platforms (36%) and leveraging intrinsic security (36%) as they expedite cloud services adoption (31%) and move a multi-cloud strategy (25%).
Takeaway: With the right digital foundation—modern, automated IT infrastructure and operations—governments can protect employee health and safety not only during work-from-home mandates but in the aftermath of natural disasters and unrest.

The pandemic highlights the need for an adaptable and resilient technology infrastructure that supports all aspects of government operations from front-office transactions and communications to back-end production and supply chains. Those agencies that had already been diversifying their infrastructure to eliminate single points of failure—moving to multi-cloud while retaining on-premises environments—were better positioned to adapt.
Strategic Insight #6

Distributed Work Capability Becomes a Business Continuity Must-Have

61% of government leaders say their organizations’ top challenge is protecting IP and data in the new remote-access world

On average, government workforces saw a 13% spike in the number of employees regularly working remotely during COVID-19. Despite some agencies already having robust teleworking policies with data protection, organizations surveyed cite three employee experience actions as priorities now. The top one is formalizing or expanding work-from-home policies (56%). Security is next: securing new endpoint risks and expanding threat management (47%). And then extend remote IT services and digital helpdesk support (42%).

This is different from manufacturing where 73% of IT and business technology decision makers place employee efficiency and workflow automation as the highest priority now. It’s also contrasted with retail, telecommunications, and healthcare leaders who believe providing employees with the physical equipment necessary to be productive remotely is their top employee experience challenge.
Takeaway: The shift to remote working was dramatic, even for government organizations used to having teleworkers, and agencies that have the most flexible and employee-friendly technology platforms are best positioned for success.

Collaborative tools, virtual infrastructure, and platforms such as the digital workspace unifying device management and identity are essential to telework success, as they enable the real-time sharing of information and users’ choice of platforms—all of which are keys to organizational agility.

Strategic Insight #7

Investment in Transformative Technologies Is Trending Up—More in Government

84% of government respondents anticipate the same or increases to budgets due to the pandemic.

More than eight in ten government respondents (84%) say they hope to stay the course—maintaining or growing annual IT spending levels—due to the crisis by continuing to invest in the adaptable technologies. A full 69% report that their 2020 IT budgets will be the same, and another 15% anticipate increases as a result of the pandemic.
In contrast, 42% of global respondents across industries only considering digital transformation but not yet implementing, are cutting budgets. This theme of digital-forward organizations preserving or increasing IT budgets plays out differently across different industries: government as well as healthcare and telecommunications providers are the most likely to maintain or increase their digital investments while manufacturing shows signs of pulling back in response to the crisis.

**Takeaway:** Leadership is increasingly in favor of IT investments that drive resilience such as speeding development and operations, enabling efficiency, and improving constituent and employee experience.

Those ahead of the curve on digital transformation investments are able to more proactively plan—and execute—their technology responses. Those businesses with tight IT budgets can first focus on optimizing infrastructure. This will help them gain sufficient efficiencies to free up the budget for digital innovation.
Strategic Insight #8
Disaster Recovery Does Not Equal Business Continuity

Just 52% of government respondents had effective business continuity plans.

COVID-19 has challenged government continuity plans. Nearly half of respondents (46%) indicate they had business-continuity plans in place prior to the crisis. However, for many, these were oriented toward traditional notions of disaster recovery. Only about half (52%) felt their plans were effective when attempting to cope with the shutdowns.

Takeaway: The pandemic is further proof that government continuity and disaster recovery (BC/DR), including COOP, strategies are critical aspects of an overall IT strategy.

BC/DR plans and technologies have traditionally been structured to support a quick return to operations as usual. Future ready organizations incorporate BC/DR into all of their operations to respond quickly to crises, adapt to new realities, and accelerate innovation. Only when government organizations can respond swiftly and effectively to crises will they be ready to make the more radical changes required for digital transformation.
Looking Forward

Keys to government agility and resilience include adaptable technology architectures, employee productivity, and forward-looking leaders, according to the MIT Technology Review study. The COVID-19 crisis is the latest—albeit most severe—test of government organizations’ abilities to respond and succeed during adverse times, and it has shown that those with future ready strategies are best positioned for success.

Understanding IT and pandemic resilience trends can help your government organization be better prepared for what’s next. To learn more visit vmware.com/go/government.