The interlocking nature of **modernization**

Digital transformation is essential to success in every government mission area, and it requires a comprehensive approach to fitting all the pieces together

The pandemic has highlighted the urgency of modernizing government systems and propelled agencies forward on their journey to digital transformation. In a recent survey of FCW readers, 71% of respondents said the pandemic had accelerated their agencies' efforts to modernize IT.

In an online article, Deloitte researchers called the pandemic "a historic pivot point for government's digital transformation. COVID-19 vaulted government headfirst into the next stage of digitization."

During the pandemic, many government activities moved online, and the public's demand for services that are convenient and easy to use but also trustworthy will only grow. Similarly, the pandemic has had a permanent impact on the workplace. The Pew Research Center conducted a survey in January that revealed a shift in the reasons for working from home, with 76% of workers saying they were working from home by choice rather than necessity, up from 60% in 2020.

To meet the demands of both customers and employees, agencies must invest in technologies and strategies that will help them achieve a truly digital government.

Cloud technology and 5G communications

A successful digital transformation has certain key elements. Agencies must be able to protect and fully utilize their data, make optimal use of cloud technology, and take advantage of the latest developments in telecommunications. Those elements are not self-contained, but interlocking and overlapping. Therefore, fitting all the pieces together requires a holistic approach.

In the FCW survey, we asked respondents which aspects of digital transformation their agencies have embraced. The most popular response at 77% was cloud computing. The next closest technology at 28% was another component of cloud: as-a-service offerings.

IDC recently forecast that total worldwide spending on cloud—hardware, software and managed

Digital Transformation by the Numbers

Sources: FCW, Gartner, IBM Center for the Business of Government

71%

FCW survey respondents who said the pandemic has accelerated their agencies' efforts to modernize IT

17%

FCW survey respondents who said their agencies apply a digital-first mindset to everything they do

75%

Enterprise-generated data that will be created and processed outside a traditional data center or cloud by 2025

$4.2 MILLION

Average cost of a data breach in 2021

services—will exceed $1.3 trillion by 2025. Furthermore, as-a-service spending will grow from 56% of total cloud spending in 2021 to 64% in 2025.

Cloud technology vendors are looking for innovative ways to meet agencies' complex demands. In addition to new technologies, they are offering flexible financial models that support agencies' ability to move between different cloud environments. Indeed, optimizing the allocation of activities between on-premises and public clouds and between multiple cloud providers has become an increasingly important modernization priority.

In addition, cloud technology relies on fast, secure communications, which means 5G has a key role to play in digital transformation. In FCW's survey, 22% of respondents said their agencies have already adopted 5G communications.

The Cybersecurity and Infrastructure Security Agency's website states that "5G will transform the digital landscape and serve as a catalyst for innovation, new markets and economic growth."

5G also enhances the government's ability to leverage data as a strategic asset for policymaking and service delivery by facilitating timely sharing and analysis of data. As networks become more widely dispersed, more of that analysis is beginning to happen at the edge.

Data protection and zero trust

Although only 18% of FCW respondents said their agencies had adopted edge computing, experts predict more widespread use of the approach in the coming years, driven by the need for real-time data analytics. Currently, "around 10% of enterprise-generated data is created and processed outside a traditional centralized data center or cloud," according to Gartner's researchers. They expect that percentage to rise dramatically to 75% by 2025.

However, they cite familiar security concerns related to hackers exploiting unsecured endpoints "in distributed denial-of-service attacks or as entry points to core networks."

Such concerns can be addressed by adopting zero trust, which rigorously and continuously authenticates users, devices and apps before allowing access to networks. The 2021 Executive Order on Improving the Nation's Cybersecurity and the Office of Management and Budget's Jan. 26 memo mandate the approach for federal agencies and set task deadlines. So far, 27% of FCW survey respondents say their agencies have adopted zero trust.

As OMB Director Shalanda Young states in Jan. 26 memo: "In the current threat environment, the federal government can no longer depend on conventional perimeter-based defenses to protect critical systems and data."

Data is a particularly attractive target for adversaries. In its annual report on the topic, the IBM Center for the Business of Government states that the average cost associated with a data breach was $4.2 million in 2021. Compromised credentials were responsible for the most breaches, but zero trust is expected to help reduce those costs.

Digital transformation also offered enhanced protection. "Organizations further along in their cloud modernization strategy contained the breach on average 77 days faster than those in the early stage of their modernization journey," the report states.

Unfortunately, ransomware is an ever-growing concern. In a Cybersecurity Advisory released in early 2022, CISA said the government "observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the defense industrial base, emergency services, food and agriculture, government facilities, and information technology sectors."

CISA offers extensive, detailed guidance for protecting against ransomware, beginning with updating operating systems and software, educating employees about the risks of suspicious email links and attachments, securing and monitoring Remote Desktop Protocol, using multifactor authentication, and making an offline backup of data.

Achieving the vision of digital transformation

In a digital-centric government, policymaking and service delivery are driven by data. The customer experience is more satisfying because it has the right balance of security and convenience. Government employees collaborate with one another seamlessly and securely regardless of location. And agencies have agile, intelligent platforms and infrastructure that support innovation in even the most challenging conditions.

Achieving that vision is a struggle for many agencies, but there are signs of progress. When asked to rank their agencies' difficulty in developing a digital-first mindset on a scale of 1 to 5, the bulk of FCW's survey respondents put themselves right in the middle.

As agencies take a more comprehensive approach to modernization, they will make rapid progress on improving public-facing and back-office operations. That progress will lead to even bigger improvements and the capacity to tackle ever-greater challenges. ■