

From emergencies to infrastructure, here's the ways government counts on cloud

As leaders and public officials rely on more cloud services, their systems must be as secure as they are reliable.

By Stephanie Susnjara | 9 minute read | August 23, 2021



Cloud offers the connectivity and security modern government demands.



Not long ago, a global landscape studded with smart cities where people live in smart homes and drive smart cars on smart roads and bridges maintained by drones and AI could only be imagined in the realm of science fiction.

Today, what was once perceived as fantasy played out in books and movies is not only becoming more of a reality—thanks to existing and emerging technology—but also the result of a global outcry for a safer, more efficient and sustainable society.

The promise of this new digitized world order came into sharp focus under COVID-19, when governments around the world raced to deliver vital public services in new ways, and to employ digital technologies at scale. Here we saw public service providers pivot quickly to furnish solutions that helped people access critical resources—whether emergency services, online education, licenses and forms or public meetings.

Now more than ever, government is relying on data and cloud technology to manage everything from its steadiest infrastructure to its most immediate crises. A digital transformation is expected to take place in our civic spaces over the next few years that would have taken a decade or more before.

Just ask Sandra Beattie, the first deputy director at the New York State Division of the Budget. As the COVID-19 pandemic unfolded last year, she was at the epicenter of the epicenter, helping dozens of crucial state and local agencies prioritize their emergency responses to a still highly mysterious pathogen. At [the Think Gov conference this year](#), she laid out one of the most aggressive and important pivots of her professional life.

[See why citizens expect modern government technology.](#) 

“When you have a national and international disaster, everybody puts aside what their priorities are, because they become aligned in a common good,” Beattie said. “It’s the first time we’ve probably ever had to have such a joint response of public health officials and finance officials working together, and the data driving the public health response was so joined at the hip of driving the response relative to the economy.”

A time for action

Whether juggling hospital staffing, school and business reopenings, public safety—especially amid protests, elections and a rise in crime—or vaccine distribution, the more connected and clear the data is, the quicker the response could be. It’s the kind of innovation and collaboration that [cloud computing](#) was made for, allowing information to be centrally located yet protected. It’s the kind of innovation and collaboration that led New York State to partner with IBM in launching the [Excelsior Pass](#), a blockchain- and cloud-based vaccine recognition system.

At the same time, the more governments and citizens come to rely on a connected society, the greater the need to keep it secure. The recent cyberattacks of both the public sector and public companies have shown just how damaging these threats can be.

“We felt that the role of technology and how that was going to play throughout the lifecycle of the pandemic—the pandemic response and the pandemic recovery—has

been at the forefront of a lot of our decision making,” Beattie said.

Government has always been at the forefront of embracing and even spurring cutting edge technologies. From the earliest calculators and computers to the space race and the foundations of the Internet, government was there.



In disasters and emergencies, data helps leaders make fast, informed decisions.

“There’s no doubt that the pandemic drove an increase in demand for government services,” Susan Wedge, IBM Public Sector market leader, said at Think Gov 2021. “Our state and local clients saw huge increases in the demand for things like unemployment claims. These clients also had to interact with its citizens in new efforts like contact tracing and vaccine management. And in all of those cases, we saw governments quickly adopt new technologies to enable their efforts.”

Harnessing cloud, AI and quantum computing is taking a bigger and bigger role in continuing to build a stronger, smarter, more connected world—while at the same time ensuring those connections are secure, protected and appropriately private. After all, bad actors have the same technological tools these days, and sometimes even better.

“It’s really about putting data at the core,” said Wedge, “and really seeing data as the resource that it is for governments to enable effective mission and service delivery.”

Emergency response is a data-driven response

In Rhode Island, decision-making based on data is helping health care officials build public trust and get vaccines to those who need it most.

“With our communities of color hardest hit, we are following the data to directly inform which are the zip codes most significantly impacted for where to focus our vaccination strategy on,” Dr. Nicole Scott, director of the Rhode Island Department of Health, said at Think 2021. “So many places around the country have had unacceptable rates of gaps in disparity in where vaccinations are occurring. And we are laser focused to use our data to close that gap.”

To coordinate its COVID-19 response efforts, the Rhode Island Department of Health worked with IBM Services to [create an operations and outreach center](#) focused on scheduling tests, delivering results and performing contact tracing. They set it all up in the span of just 12 days in September 2020. This increased the speed of case investigations by five times and provided predictive insights used to guide state-level public health communications messaging. The contact center optimization [allowed schools to remain open](#).

On the other side of the globe, Australia took a war room approach to its vaccine roll out with fast cloud computing implementation that utilized [IBM’s hybrid-cloud approach](#).

“We started to scale existing infrastructure but there came a point in time when we just needed to make a decision,” Derek Byrnes, national manager at Services Australia, said at Think. “Our legacy mainframe was not designed to scale for this challenge and we chose to go to cloud, which was a bold decision.”

Yet if the public is to trust these powerful new technologies, they must be open and transparent and made secure through widespread monitoring, especially as we rely on tech for more and more.

Alarm bells are becoming more prevalent every day. Take the SolarWinds hack, the [shutdown](#) of one of America’s biggest fuel pipelines and ransomware hitting major banks, food processors and other critical businesses. These are all clear demonstrations of the consequences of failing to strengthen cybersecurity at critical infrastructure facilities. The Biden Administration is hitting back, with a [new executive order](#) to improve the nation’s cybersecurity.

Using tech to build tech resilience

Here's the rub: the more complex and layered tech infrastructure becomes, the more holes there are for attacks. We need that complexity for society to continue to progress. We also need to make sure it's secure because we're so dependent on it.

“Complexity is the enemy of security,” Howard Boville, head of the IBM Cloud Platform business at Think Gov 2021. “Some companies are forced to put together as many as 50 different security solutions from up to 10 different vendors to protect their sprawling technology estates. Every node in these fantastically complicated networks is like a door or window that might be inadvertently left open. Each represents a potential point of failure and an exponential increase in cybersecurity debt.”

While criminal-based ransomware and external attacks are a huge concern and get the most media attention, they are not the only threats to be aware of in a digitized world. Malicious insiders and human error also account for cybersecurity issues.

Predictive AI built on the cloud can help clear all kinds of bottlenecks.

The events of 2020 accelerated many organizations efforts to converge their information technology (IT) with their operational technology (OT). For those unfamiliar, OT monitors and manages asset for industrial or civil engineering equipment. And as these systems have become more digitally connected, they also become more vulnerable.

“Computerized operation technology is grossly under-treated as a risk,” said Marty Edwards, vice president of Operational Technology Security at Tenable, a cyber exposure consultancy, at Think 2021.

“We spend millions of dollars on national and critical infrastructures but we treat operational technology like they are an extra piece instead of really focusing in on them and giving them the care and attention they deserve.”

It all boils down to [a connected, secure cloud environment](#) that embraces zero trust architecture across the enterprise.

As government and public institutions move further and further away from the industrial control systems of yesterday and more toward cloud solutions, an opportunity is created simultaneously to address security vulnerabilities. This can be seen in action in the civil infrastructure industry, which in some countries, is on the brink of a digital renaissance.

Reimagining Civil Infrastructure Asset Management

The magnitude of costs attached to civil infrastructure is staggering, given how asset- and labor-intensive it is to maintain bridges, tunnels, ports, roads, rails, utilities, airports and transport. For instance, 2 billion man-hours are spent yearly on manual inspection of bridges alone.

There's another way.

“We are moving from time-based to predictive maintenance,” Mikkel Hemmingsen, CEO of Sund & Bælt Holding, explained at Think 2021. “This is the same digital journey as the airlines who ask, ‘What is the condition of our engine?’ We must ask, “What is the condition of our concrete, etc.”

His company's mission is to build, operate and finance infrastructure, including large tunnels and bridges that connect Denmark, Sweden and Germany. Sund & Bælt recognizes that smarter infrastructure is not only better for workers, assets and the bottom line—it's also better for the planet.

To that end, [Sund & Bælt worked with IBM to create an AI-powered IoT system](#) that uses sensors and algorithms to help prolong the lifespan of aging bridges, tunnels, highways and railways.

“A great bridge was designed to last 100 years,” Hemmingsen said. “If the lifetime of the bridge is now 200 years, we have halved our carbon footprint.”

In Italy, road operator [Autostrade per l'Italia is working on a revolutionary platform](#) which also uses IBM's AI-based Maximo software platform to boost efficiency and transparency of structural analysis of its properties. Digital twins, drones with laser cameras and inspectors and technicians with mobile devices are just some of the tools now working in the field.

“To introduce digital asset management it is important to have a clear goal and develop a trial-and-error process, accepting you don't have the completely standardized product,” Roberto Tomasi, CEO of Autostrade per l'Italia, said.

Shaping A Smarter Future

The digital transformation happening across the public sector—spurred further by the challenges of COVID—offer a guide for a smarter global society where technology can strengthen economies, make institutions more effective, increase equity and improve citizens' well-being overall.

“We have an unprecedented opportunity and responsibility to update the architectural foundations of our digital infrastructure and pay off our cybersecurity debt,” Boville said. “I believe that with the right measures—a strong public and private collaboration—we have an opportunity to construct a future that brings forward the combined power of security and technological advancement built on trust.”

[Want to join a community of industry leaders and tech experts sharing ideas like this? Discover more.](#)



Read More



How tomorrow's quantum computing raises cybersecurity risks today

by James Daly





Why modernizing government technology was a necessity even before COVID-19

by James Daly



A big little problem: How to solve the semiconductor shortage

by James Daly

Categories

Cloud

Government

Deep Dive

Also of Interest:

In Ecuador, sustainable shrimp for a sustainable...

IBM's Sarah Diamond is helping banks transform...

How 5G boosts smart factories, smart cities and...

Banking on data to disrupt human trafficking