

# The role of networks in delivering government digital services



Caribbean governments, along with large enterprises, are poised to enter a new digital age. Recent advances, like cloud computing, the Internet of Things (IoT), data analytics, and social media, are changing how they deliver their services. The evolution promises to streamline processes, lower costs, and improve citizen satisfaction. However, in many cases, the change will only be effective if government agencies also upgrade their network infrastructure.

Delivering government services can be a difficult, time-consuming, and manually intensive process. Strict governance requirements and policies sometimes mean workers spend their time simply keeping systems and processes running, rather than simplifying them for both constituents and employees.

## New network requirements emerge

Recent dramatic changes unfolded on a few fronts. The pandemic forced agencies to move workers out from central sites to remote locations. Therefore, they needed new tools and network connections to complete their work—and complete it securely.

The Internet of Things (IoT) shrunk computer processing power down into small sensors that can be placed in new locations.

Smart cities are gaining attention because they have the ability to provide more insight into how agency services perform, simplify delivery processes, and enhance citizen satisfaction.

New applications are emerging. Increasingly, cities are deploying surveillance cameras to oversee traffic conditions, keep the streets safe, and respond to emergencies.

In sum, as cities adopt these advanced tools, workload requirements grow, driven by the increasing complexity.

## The need for reliable network infrastructure increases

As the internet, digital, and cloud solutions become essential dependencies to power applications, many government agencies realise they have 20th-century networks that simply cannot support their 21st-century applications. Problems arise on many fronts:

- Routine chores, like implementing software patches and updates, overwhelm the network and slow system performance to a crawl.
- Agencies lack the ability to scale effectively as they expand system capabilities.
- Costs rise as they extend government offices to new localities.
- Security challenges increase as network services become more complex.
- Equipment often has to be manually upgraded because the systems support little to no automation.
- Network management is conducted in a siloed manner, so a lot of time is spent on data consolidation. This leads to inefficiencies such as duplicate reporting and bureaucratic hurdles.
- State and local governments face competition for the network talent required to keep up with demand.
- As a multitude of new endpoints are connected to their distributed network, the attack surface becomes broader and more complex to manage.

Compounding the problem, the government works with multiple vendors and may have deployed best-of-breed piecemeal solutions. Managing the disparate pieces on their own intensifies the IT burden, raises costs, and increases the risk of errors, poor performance, and downtime.

## Time to evaluate network options

Such issues have intensified as digital transformation has taken root. In this increasingly complex environment, it's important for governments to take a step back and examine their network operations end-to-end. Service delivery improvements require enhanced performance and productivity, continued cost-efficiency and upscaled monitoring and security processes. Many agencies find that their existing networks cannot meet these challenges.

They can improve their position by upgrading their existing system. Emerging solutions, like Software Defined Wide Area Networks (SD-WAN), enable governments to connect multiple locations with high bandwidth networks, lower their costs, and ensure secure connections.

Such a transformation is grounded in a more intelligent approach to networking. The network is no longer based on legacy, physical hardware components that require significant manual input. Instead, it becomes a cluster of virtual devices controlled by intelligent software. They gain simplified, centralised management of critical network functions, reducing equipment costs, shortening provision times, and improving traffic management.

In addition, new networks include high levels of automation, so any network changes are seamlessly translated across all IT environments. Automation also features one-touch security policy updates that are enforced at all ingress and egress points, streamlining critical system monitoring and reporting.

Cost is another plus. Local and state governments connect operations directly to the internet for less expensive gigabit broadband circuits, in certain cases receiving ten times or more bandwidth than they had previously.

Security becomes tighter. New networks include built-in security features, such as firewalls, that empower governments to connect employees to software applications—whether they're in the office, a coffee shop, or an airport lounge—while preventing unauthorised access and keeping the data safe.

Nowadays, governments recognise that the network is a critical component of their digital transformation. Therefore, it is important to make it a strategic priority rather than an afterthought. New networks streamline communications, scale, lower costs, and improve performance, providing citizens, employees, and partners with more satisfying experiences.



## Call in a network expert

For government agencies looking to achieve their public missions in an increasingly digital landscape, network transformation is as critical as digital transformation. However, it is a daunting prospect, one fraught with many choices.

Given their vast portfolios, governments often face challenges in allocating sufficient time and expertise toward navigating their options, making informed choices, and monitoring their network infrastructure. Third parties are able to take on that work. These network experts have deployed solutions for many Caribbean agencies, are experts in different products, have sophisticated control centres, and established best practices.

At C&W Business, we leverage our global expertise to address the unique local challenges faced by government agencies in upgrading their network infrastructure. As a trusted partner in the Caribbean region, we have the experience and expertise to help governments navigate their network options and deploy the right solutions to support their digital transformation initiatives.

With C&W Business as their partner, government agencies can focus on their public missions while we take care of their network infrastructure.

At **C&W Business**, we're your catalyst for transformative success. From Cybersecurity to Cloud, Data Centres, Unified Communications, and Connectivity, our streamlined solutions ensure scalability and security. With the Pan-Caribbean region's largest and most reliable network. We unleash the digital future of the Caribbean society.