The new realities driving government network transformation

verizon

Contents

Introduction

Every day, millions of people in states, cities and rural areas throughout Australia rely on network connectivity to execute critical tasks in their lives.

A business owner relies on it to process customer transactions or to apply for a new local government grant. A first responder needs it to get timely information about what awaits her at the scene of a massive accident. A state health department employee depends on it as he wades through information to make an eligibility determination that could make all the difference for a family in need. And for a student whose university is using technology to enhance off-campus learning, strong network connectivity could determine whether she can participate in the day's lesson plan or fall behind.

Though we often don't fully realise it, network connectivity serves as a critical lifeline for so many communities. It's not just about downloading the latest viral video or being able to send a text that arrives in milliseconds. As the COVID-19 pandemic made all too evident, network connectivity enables so many aspects of government service delivery that when networks falter or don't function optimally, the consequences could be significantly disruptive and potentially catastrophic.

The ability to implement a modernised, secure and resilient network in government is often challenged by outdated resources and budget realities.

As governments work to become more technology-enabled, they'll not only need to enact digital transformation but also network transformation.

Network transformation can drive better government in six key areas:

1. **Core technologies:**
   Automating and modernising legacy systems

2. **Workforce:**
   Delivering a better employee experience

3. **Cybersecurity:**
   Securing the new edge

4. **Public safety:**
   Protecting communities and improving emergency response

5. **Connectivity and access:**
   Closing the digital divide

6. **Budget and cost control:**
   Optimising various funding streams and improving financial sustainability

With network transformation, governments can deliver a better constituent experience, make meaningful progress toward achieving their mission and finally realise the vision of digital government. This report provides a roadmap for how they can start and successfully navigate this journey.

What is network transformation?

Network transformation means modernising an organisation's network architecture to accelerate the delivery of information, improve application and system performance and optimise scale and reach.

In terms of government service delivery, "network transformation is about strategically re-evaluating your network architecture, then implementing new technologies and processes to enable more effective and efficient services for citizens," says Rabi Roil, ANZ Senior 5G Solutions Engineer at Verizon Business. "This means putting your organisation and its infrastructure under a microscope and making decisions about what you want it to be able to do in the future."

This kind of transformation forces governments to focus on the outcomes they want to achieve. But at a more granular level, it drives them to carefully think about their approach to network design. In a digital world, network design must be more hyperdynamic and interconnected, with the ability to assign roles based on defined business criteria rather than just an IP address.

"Network transformation involves moving away from a diverse array of point products and services and applications with little common oversight to an ecosystem of applications and capabilities that work more collaboratively," says Tony Harb, ANZ Head of Solutions Architects at Verizon Business.

To achieve network transformation, governments first need a deeper understanding of the citizen experience and how residents interact with various agencies and departments across the ecosystem. Citizens now judge their interactions with government agencies based on the customer experience they receive in the private sector. They expect real-time, responsive, personalised service, but governments historically haven't been well equipped or sufficiently resourced to meet these expectations.

In some respects, the pandemic illuminated these issues but also accelerated progress toward resolving them, as governments everywhere implemented virtual services, with the help of a variety of cloud-based software-as-a-service applications, to streamline service delivery and bolster their resilience.

Public sector organisations scrambled to implement videoconferencing, digital workspaces and distance learning platforms, but they often failed to consider efforts to strengthen network connectivity in the long term.

[1] https://www.theguardian.com/australia-news/2022/dec/13/digital-divide-report-finds-some-australian-rural-mobile-data-speeds-90-slower-than-urban

[2] https://www.abc.net.au/news/2022-10-16/australia-digital-divide-millions-cannot-access-internet/101498042

Many local governments face ongoing connectivity challenges that boil down to affordability and infrastructure issues, and continue to grapple with legacy technologies and on-premises environments that aren't always compatible with modern connectivity solutions. Accessibility is another pressing challenge. A study by RMIT University found that while 91% of Australians are active internet users, metropolitan access and performance remains significantly higher than in regional areas. RMIT Professor Mark Gregory said that mobile data speeds in rural towns were 90% slower on average than those in urban areas .

This 'digital divide' means 2.8 million Australians remain 'highly excluded' from internet access. "It's limiting people's ability to participate in society and access services that they need for their lives – we're talking about some of the vulnerable, low-income people in the country not able to access the services designed to assist them", said RMIT University researcher Daniel Featherstone .

As these figures make clear, network transformation is crucial for enabling governments and the constituents they serve to access modern digital applications for activities including hybrid work, distance learning and digital service delivery. Network transformation is also critical to advance key goals such as digital equity, increased public safety, and economic growth and development.

This transformation can be a crucial catalyst for governments as they try to achieve these strategic objectives. To kickstart both their digital and network transformations, government organisations can begin by focusing on modernising their core technologies.

2.8 million

Australians remain highly excluded from internet access

1 / Core technologies

Driving automation & legacy system modernisation

Network transformation is inextricably linked to digital transformation. For governments to become more agile and deliver better and faster service, they need to modernise legacy networks and redesign their network architecture.

The traditional approach to networking in the public sector has typically relied on a hub-and-spoke model with branch sites connected to a centralised data centre via a router over public or private fibre, Ethernet or multiprotocol label switching (MPLS) connections. Within this network architecture, traffic is routed based on IP address rather than business priorities, which means data from mission-critical applications often isn't routed as quickly as it should be.

Traditional government networks weren't built to handle the massive bandwidth requirements associated with thousands of employees working remotely or multiple agencies using cloud, Internet of Things (IoT)-based and artificial intelligence (AI)-driven applications. But the world has changed, and government networks must change along with it to support these use cases and other emerging needs within government operations. To accelerate network transformation, governments must transition from legacy networks to software-defined networks that are better able to meet the bandwidth and performance demands, low latency and high availability requirements necessary to run a digitally driven organisation.

Roil says software-defined wide area networking (SD-WAN), multi-access edge computing (MEC), secure access service edge (SASE) and 5G are some of the foundational technologies governments need to enact network transformation.

SD-WAN is a virtualised networking technology that overlays MPLS and/or internet circuits, routing low-priority network traffic over less expensive circuits and prioritising the delivery of data from mission-critical applications to ensure lower latency, better

performance and high availability. Government organisations can implement this technology on their own or use SD-WAN managed services to drive more value from this investment. With MEC, data is stored and processed as close to its intended destination as possible, while 5G is fifth-generation wireless technology that uses low, mid and high-band radio frequencies to increase network capacity. 5G also enables the network to better support latency-sensitive, high-bandwidth applications.

"If you have SD-WAN with network function virtualisation [or software based, rather than hardware-based network services], then you really have the best of both worlds," Roil says.

Roil adds that MEC takes an organisation's compute environment and moves it closer to its user community, which is critical for the optimal delivery of voice and video data transmissions. He says one of the capabilities that makes 5G so valuable is that it enables network slicing, a network architecture that allows multiple software-defined networks to use the same physical network infrastructure. With network slicing, government organisations can create isolated and defined networks designed to meet a specific use case or application requirement, whether it's powering an unemployment claims system, business permitting application or video surveillance system for police investigations.

"The application always gets the bandwidth. It always knows that it has a transmission path because it is that impactful to the organisation," Roil says.

By redesigning their network architecture around software rather than hardware-based connectivity solutions, governments can position themselves to integrate cloud and AI-driven technologies that automate their processes and increase data visibility and accessibility throughout their organisations.

Once they lay this foundation, governments can put their network to work for a variety of mission-critical use cases, such as initiatives that improve the employee experience and lead to workforce transformation.

With network slicing, government organisations can create isolated and defined networks that are designed to meet a specific use case.

2 / Workforce:

Delivering a better employee experience

Even before the pandemic, government agencies were gradually moving to the cloud. However, the public health crisis accelerated cloud migration and the need for these organisations to modernise their networks as employees' homes become the new perimeter. Harb says network transformation can help governments increase their agility in several ways.

One of the most urgent factors driving network transformation is today's hybrid work environment. Government facilities may have to redesign their network architecture to support a new remote work infrastructure that encompasses solutions such as videoconferencing systems, digital collaboration platforms, cloud-based document management systems and IT asset management tools. They'll also need to enact network transformation to expand connectivity for residents throughout their local area, says Harb.

"Employees expect a fully hybrid work environment, so how do you manage the return-to-work aspects from an economic perspective as cities look to keep those revenue streams going?" Harb says. "5G can enable things like internet connectivity for employees on mass transit systems, so they can be productive while going into the office."

Both Harb and Roil say that although governments at all levels must focus on the technological aspects of network transformation, effective change management is just as critical. They say leaders need to start with a clear vision and goals, revamp their business processes to reflect behavioural changes that often come with remote work, and develop digital skills training to effectively use the tools they've implemented.

"For organisational change management, I usually think of three big things: communications, behaviour change and training," Roil says. "You need to have leadership support for it and communicate to employees why it's important for your organisation to enable everyone to work from home — the goals behind it and the vision behind it. You also need immediate managers communicating out the message about how this is going to impact their specific employees."

Network transformation will pave the way for workforce transformation in government. As governments prepare for the future of work, they can bring their people, processes and technology together to empower employees, streamline and automate routine and repetitive tasks, and better align their work with their organisation's overall mission.

Government facilities may have to redesign their network architecture to support a new remote work infrastructure that encompasses solutions such as videoconferencing systems, digital collaboration platforms, cloud-based document management systems and IT asset management tools.

3 / Public safety:

Protecting communities & improving emergency response

Public safety agencies rely on technology to keep their communities safe, from geographic information system (GIS) spatial information tools, drones and radio communications technologies to data management and evidence collection systems.

However, reliable connectivity continues to be a challenge for these departments. With ongoing calls for accountability within law enforcement, network transformation can help first responders and law enforcement professionals improve public safety and their interactions with the public.

Roil says robust network connectivity has several applications in public safety. It can make it easier to safely collect, store and analyse data from body-worn cameras, crime tips and evidence generated from the public via social media. It can also accelerate information delivery from an emergency dispatch centre to officers in the field to improve situational awareness when they respond to a crime scene.

"Public safety remains top-of-mind for Australians in light of multiple emergency situations over recent years - including bushfires, flooding and COVID," says Roil. "It's become really important for emergency services to have an open dialogue with the constituents they support. That will increase trust, reliability and relationships as we go forward. Technology is at the forefront of making that happen."

Network transformation can also support purpose-built applications that are specifically designed for public safety and law enforcement agencies, such as heart monitoring technologies that will enable first responders to share information in near real-time with hospitals as they transport patients. Or smart, IoT-enabled helmets that increase firefighters' field of vision in zero- or low visibility situations.

With better networks, first responders can take advantage of 5G-enabled unified communications platforms that ensure their communications are highly secure and prioritised for rapid delivery across the network. Advanced network technologies can also help ensure public safety agencies' communications infrastructure is highly available, reliable and resilient — as long as the network is built with redundancy in mind and incorporates battery and satellite backups to reduce the risk of network failures.

Some municipal departments in the United States have already implemented network modernisation to improve emergency response operations. For example, a large water utility in western U.S., which supplies water to firefighters, leveraged 4G LTE networks, a dedicated mobile app with real-time connectivity and smartphone devices purpose-built for hazardous environments to maintain communications with firefighters in remote areas as they battled wildfires.

Implementing these advanced network connectivity solutions has allowed the utility to improve the delivery of water resources, enhance interoperability across devices so the agency and firefighters can communicate across both phones and radios, and help ensure worker safety with communications that meet occupational health and safety requirements.

Network transformation will enable public safety departments to communicate more effectively, not only with their own resources, but with all of those who are part of the response recovery efforts. It will also enable quicker and smarter decisions.

As government departments modernise their networks, Harb says it's important to remember there's no one-size-fits-all approach to network transformation. For example, emergency services may still be able to make good use out of various public safety technologies with 4G connectivity, rather than 5G.

"You're only enhancing your network — you're not eliminating it," Harb says. "With network transformation, it's about really understanding where you want to go and knowing that 5G may not be the answer for everything, but it might be the answer for a lot of things."

A large water utility in the U.S. leveraged 4G LTE networks, a dedicated mobile app with real-time connectivity and smartphone devices purpose-built for hazardous environments to maintain communications with firefighters in remote areas as they battled wildfires.

4 / Connectivity & access:

Closing the digital divide

In regional and rural communities where there may be limited funding, fewer fibre lines and less associated infrastructure to expand network capabilities, governments all over the world are being challenged to devise a different plan for network modernisation.

There are three primary drivers for digital inequality: geography, socioeconomics, and technology. In the United States, this is being addressed with a whole-of-state approach to network transformation, building on what's proved an effective model for cybersecurity. Federal stimulus relief — including the American Rescue Plan Act — and other federal broadband funding streams have given states a prime opportunity to make these investments in rural areas. They've also lowered some of the cost barriers for network providers who have not yet expanded in these locations because they're difficult to reach or have rugged terrain[3].

Income and social disparities mean 42 million Americans lack broadband access, and 33 million can only access dial-up or DSL connections. The resulting limitation in access to new digital service provision, education and professional opportunities has prompted the Affordable Connectivity Program[4].

Technological drivers include unequal access to satellite internet coverage, and new solutions including 5G and private 5G fixed wireless access (FWA) and millimetre-wave FWA (mmWave FWA).

In Australia, the geography and funding models may be different, but the federal government has the same goal of avoiding a digital divide.

"Some communities don't have access to the face-to-face services that towns would have, for instance, a Centrelink office or a bank or a post office. They need to access them online," notes RMIT University's Daniel Featherstone[5]. Australia's sheer size and the remote access requirements for indigenous, defence, mining and other bodies mean that a combination of technologies including the National Broadband Network (NBN), public and private satellite and private 5G may be required.

Publicly-supported solutions to address the digital divide aren't just a question of connectivity. Public authorities also have a key role in defining cybersecurity standards such as the Australian Signals Directorate's Essential 8 or Information Security Manual (ISM), to protect their citizens' digital migration and sensitive data.

Publicly-supported solutions to address the digital divide aren't just a question of connectivity. Public authorities also have a key role in defining cybersecurity standards such as the Australian Signals Directorate's Essential 8 or Information Security Manual (ISM), to protect their citizens' digital migration and sensitive data.

[3] https://www.brookings.edu/blog/up-front/2021/08/18/the-benefits-and-costs-of-broadband-expansion/

[4] Solving America's Digital Divide; Kevon Ross, 19.08.22; https://www.forbes.com/sites/forbestechcouncil/2022/08/19/solving-americas-digital-divide/?sh=51e1b7c03de8

[5] https://www.theguardian.com/australia-news/2022/dec/13/digital-divide-report-finds-some-australian-rural-mobile-data-speeds-90-slower-than-urban

5 / Cybersecurity:

Securing the new edge

Regardless of whether federal, state and local governments improve network connectivity to transform their workforces, enhance public safety or advance digital equity, they must make sure their networks are secure.

As public sector organisations introduce new applications and technologies into their IT environments, they expand their attack surface. In 2020, in the US, cybercriminals targeted nearly 2,400 governments, schools and health care facilities with ransomware attacks . In addition, denial-of-service attacks, malware, phishing and other social engineering schemes continue to be persistent threats for governments.

In this threat environment, governments need to be laser-focused on endpoint and network security to ensure business continuity and to help avoid a massive security breach that could undermine the public's trust and increase their organisation's regulatory risks. Roil says network transformation gives all levels of government the opportunity to strengthen their security posture.

"When you step back and analyse your network infrastructure strategically, it gives you an opportunity to look broadly at all the pieces of the puzzle. That includes your security operations and how well they're integrated into network visibility," he says.

Roil says incorporating network detection and response (NDR) tools into their security strategy can help governments as they undergo network-driven digital transformation. These tools capture massive amounts of network traffic, identify security gaps and anomalies in an organisation's IT environment, and enable proactive threat hunting. As a managed service, governments can leverage NDR technologies for security automation and orchestration, relieving some of the burden on their IT teams and redeploying these resources to other digital transformation initiatives beyond just network management.

If an organisation is looking for a security framework to follow as it navigates network transformation, Roil suggests the SASE model, which integrates SD-WAN and other cloud security approaches.

"SASE extends security to network transformation. It's a great opportunity to bring together capabilities like SD-WAN, secure web gateway, software-defined perimeter and Zero Trust, which assumes that a device doesn't belong on the network and constantly validates that it does," he says.

As governments modernise both their networks and IT assets, they'll need to continually assess their security risks. No organisation will ever have the resources to combat every threat. But by better understanding the specific threats they face, making security investments that are proportional to their organisations' unique risks and employing NDR tools for enhanced network security, governments at all levels can significantly reduce their risk profile.

As public sector organisations introduce new applications and technologies into their IT environments, they expand their attack surface.

6 / Budget & cost control:

Optimising funding & improving financial sustainability

Any transformation, whether digital or network-based, will come at a cost to government organisations.

Though there are upfront costs with modernising network architectures, the long-term return on investment is invaluable.

For one, network transformation makes it easier for governments to implement advanced security tools, like NDR technologies or AI-driven security automation platforms. Considering the average cost of a data breach now tops AUD $4.03 million[7], this cost avoidance alone can help governments achieve better cost control.

"The immediate saving is that you're less likely to be a target of a ransomware attack," Verizon's Harb says.

There's also the hard-to-quantify cost and time savings associated with automation and increased employee productivity, along with the more tangible costs associated with better IT asset management, such as reducing licensing fees and vendor lock-in.

Harb says network transformation makes it easier for government organisations to right-size their IT environments, enabling them to implement best-of-breed solutions without a heavy IT lift and retire legacy applications that no longer serve their needs.

Though network transformation will be an ongoing process for many government organisations, Harb says employing a network-as-a-service approach is one of the best ways governments can cost-effectively modernise.

Network providers like Verizon often work with government agencies to deploy technologies as an operating expense rather than a capital expense, so it becomes a monthly cost. This approach also allows agencies to benefit from unified network management, since a suite of interoperable network connectivity and security tools function together as part of this service.

Going forward, governments will need to increase their resilience. Network transformation will be a key part of this effort. Tapping into current federal funding streams, working collaboratively with network providers, and potentially adopting a service-based approach to network security and management can put governments on a sustainable path toward modernisation.

The long-term return on investment is invaluable.

[7] https://australiancybersecuritymagazine.com.au/average-cost-of-a-data-breach-in-australia-up-32/#:~:text=IBM%20has%20released%20key%20Australian,according%20to%20the%20report%20findings.

Best practices for network transformation

As local, state and federal governments look to enact network transformation, they should consider using a framework called "The Five States of Ready[8]" to help them navigate their modernisation journey.

The Five States of Ready

1 Start

An agency or government should begin by identifying their core business needs, align them to key strategic initiatives and then identify technology partners who can put them on the path to modernisation.

Harb says when assessing technology partners, governments should "look for a provider that can start at the end and help the organisation refine its vision, articulate what it wants to be, understand what the possibilities are, and not just look at the engagement as a technology implementation, but as a partnership.

"When you talk about digital transformation in government, you're essentially talking about changing society to a certain degree — whether it's smart cities, drones or driverless cars to improve public transportation," Harb adds. "The possibilities really are endless, especially with 5G, but they require vision and a partner who can help organisations get there."

2 Adapt

Once agencies identify their needs and choose a technology partner, they can begin to implement and test secure, interoperable network connectivity solutions that enable them to be more agile and efficient and drive better performance.

For all levels of government, these solutions may include some of the core technologies previously outlined, including SD-WAN and managed network services. Implementing these technologies can also help public sector organisations better understand and deploy their data for a range of use cases, whether it be hybrid work, emergency response communications or digital service delivery.

[8] https://enterprise.verizon.com/resources/whitepapers/digital-transformation-strategy-for-public-sector/

3 Elevate

At this stage, organisations will start making better use of the data flowing into their networks. They'll capture it at scale and begin to use it to inform their decision-making to drive better outcomes.

In government, this could mean uncovering insights that lead to the implementation of self-service tools to reduce call centre wait times or pinpointing which intervention programs are most effective at reducing juvenile interactions with the criminal justice system, and therefore doubling down on these efforts.

4 Innovate

At this advanced stage, an agency will have evolved into a more data-driven organisation and its network architecture will be optimised to deliver on its evolving business needs. It will likely be using AI to drive the interconnectedness of data, people and processes and for intelligent decision-making.

At the "innovate state of ready," governments will also move from a reactive stance to a proactive approach where they are more equipped to anticipate constituents' needs and that of their own workforce. What does this look like in the real world? IoT-enabled communications on public transit, digital kiosks that deliver timely alerts in public spaces, and real-time response systems that increase situational awareness for first responders minutes before they arrive on scene — just to name a few.

5 Adapt

This end state isn't just aspirational — it's achievable.

At this stage, governments will be well equipped to adopt the latest technologies to create a more responsive and agile operating model. They'll be better positioned to make changes that truly improve residents' quality of life and drive business and economic growth, and SASE, 5G and MEC will be a core part of their network design. Modern connectivity will bring to life smart city initiatives and digital interfaces and applications largely will be the first touchpoint through which constituents interact with government — ultimately making real the promise of digital government.

Conclusion

Network transformation is the backbone of digital transformation, but to start on this journey, governments must be intentional in their approach.

Over the last two years, governments have had to rapidly adapt. They haven't had sufficient time to assess what a future-ready network architecture really looks like. Though governments have made gradual improvements to their network and IT infrastructure in recent years, now is the time for them to make lasting and impactful strategic investments.

With the rapid shift to the cloud, increased calls for digital equity and a relentless threat environment that makes holistic cybersecurity more vital, governments must establish a strong foundation for reliable, high performing network connectivity. There's never been a more critical time to do this, because, as Harb says, "what we've learned during the pandemic is that quality connectivity is no longer 'nice to have' — it's essential."

This handbook was created by InnovationAus.com, with information and input from Verizon.

verizon