Wildfires, Natural Disasters & Network Resilience

By Ryan Johnston

Next Century Cities

FIND MORE RESOURCES AT BROADBANDHUB.ORG

OCTOBER 2023

The United States is no stranger to wildfires. So far this year CalFire has logged over 3,300 wildfires and over 12,500 acres burned. These fires can ignite utility poles, melt aerial fiber optic cables, obscure wireless signals, or damage transmitting or receiving equipment. This kind of damage can cut homes off from key public safety resources, and prevent calls for help in the most dire situations.

As states now know their share of the $42.5 billion Broadband, Equity, Access, and Deployment ("BEAD") program, they should begin planning new network deployments and upgrades to withstand increasingly severe natural disasters.

Network resilience refers to a network's ability to withstand and recover from an unexpected event or disruption while maintaining a reliable level of connectivity to the user. Network administrators put plans in place to address a range of events, from wildfires and floods to cyber-attacks and hardware failures.

States and localities are not the only ones that should take proactive planning measures to ensure new and existing telecommunications and broadband networks are resilient. Providers and other network operators should upgrade equipment or ensure that proper backups are in place to mitigate future outages before a disaster strikes a community.

What's more, resilience planning requires collaboration at every level of government. Local and state officials should partner with the private sector to highlight potential failure points and critical redundancy measures. By taking a few simple steps to enhance communication and planning, both governments and providers can ensure that consumers maintain connectivity during and in the wake of natural disasters when they need it the most.

1. Providers Should Replace Aging or Outdated Network Infrastructure.

Once a disaster strikes and network outages have occurred, it is too late for a provider to determine that it should address its aging or outdated network infrastructure. For example, in the aftermath of superstorm Sandy, New York City found that longer-term communications outages were caused by flood damage to commercial and residential buildings and, specifically, to the internal or external telecommunications hardware attached to those buildings. As a result, the City began to use the renewal of franchise agreements with cable providers to establish standards for repair timeliness and data reporting and publishing requirements.

Before franchise agreements were up for renegotiation, the City encouraged providers to increase disaster preparedness and also required providers to submit business continuity plans which must be updated on a regular basis. Taking a proactive approach, identifying and either replacing or hardening aging infrastructure before disaster strikes may be the difference between residents remaining online or being left in the dark.

2. Collaborating with State and Local Governments Helps Providers Address Regional Nuances.

The threats in each region of the United States vary. While the West Coast is dealing with long-term wildfires, the Gulf Coast may be gearing up for a particularly difficult hurricane season, or the Midwest might be experiencing significant superstorms leading to increased tornado activity. Proactive collaboration between state and local governments with their Internet service providers can provide critical asset information while allowing planning for the incredibly diverse geographic and topographical challenges.

Early collaborative planning efforts open crucial communications channels which can expedite repair coordination, emergency services deployment, and resource mobilization efforts. When governmental partners and providers can streamline disaster response efforts when both have a clear understanding of what roles each stakeholder will play before, during, and after a disaster.

3. Federal lawmakers and the Federal Communications Commission should promote information sharing and develop benchmarks for resilience planning.

Currently, the Federal Communications Commission ("FCC") only collects data regarding network status and situational awareness on a voluntary basis. Providers are not required to share with the FCC how networks are performing during natural disasters and even if outages have significantly impacted the performance of broadband networks. Under the reporting requirements for the National Outage Reporting System ("NORS") the FCC collects outage data as it relates to disruptions to telephone service, not broadband.

Providers are not required to share with the FCC how networks are performing during natural disasters and even if outages have significantly impacted the - performance of broadband networks.

In addition to the limited data the FCC collects, access to the information by state and local agencies requires a potentially onerous attestation process that promises to keep outage information confidential. communities recovering from disaster. The lack of transparency keeps state and local governments on the back foot while they try to determine who is disconnected and how to coordinate recovery efforts.

Additionally, funding is often the largest barrier to adopting network resilience programs at the local level. Hiring consultants, conducting research, and building infrastructure and the manpower required to launch emergency planning programs introduce financial burdens that many localities cannot bear.

Both Congress and the FCC have agreed that resilience planning is essential, and the Government Accountability Office has identified several avenues through which the federal government can make resilience funding available. There is no excuse to delay overhauling the federal approach to disaster recovery, especially when providing every resident with reliable broadband connectivity is an express goal from every level of government.

NUMBER OF BILLION-DOLLAR NATURAL DISASTER EVENTS 1980-2021