The Five Capabilities Required for Disaster Communications

verizon

A disaster rips away a community's security and well-being, putting lives and property at risk. Citizens look to federal, state and local authorities for help – both from immediate danger and for assistance in piecing their lives back together. The most basic and sacred government responsibility is to protect the public. That means that every calamity has the potential to be, in the words of Winston Churchill, government's "finest hour."

But government can't do it alone. At all levels, government needs a public safety partner with the resources to help save lives, minimize property damage and restore normalcy to affected communities.

Many public safety organizations are being asked to choose a network provider to rely on in a crisis. To evaluate the right partner, it is important to understand the five communication capabilities for effective disaster recovery:

- Situational Awareness
- Security
- Connectivity
- Mobility
- The Network

Situational Awareness

When you are part of a team that responds to a crisis, without situational awareness you're running blind. In the aftermath of a disaster, first responders need infrastructure and technology that identifies potential resources on the scene – their location, technology capabilities and personnel credentials. This includes fire and rescue, law enforcement, medical personnel and recovery teams. Those responding to a crisis can even include private citizens with their smartphones and a boat or vehicle.

STRIPE for Crisis Management

"A term I use to capture what is necessary is STRIPE – a Space, Time, Role, Identity and Persona Environment," said Jeffrey Schweitzer, asymmetric solutions architect at Verizon. "In the world of first responders, this allows command to deploy the right resource with the right equipment and the right skills to the right problem at the right time. This encompasses any and all resources – for example, how the 'Cajun Navy' coordinated help for victims of Hurricane Florence."

Crisis management starts with a common operating picture of the field. Effective disaster response requires detailed organization based on real-time information, including availability of assets, location of resources by type, solutions for information sharing and the ability to communicate and collaborate.

Collecting the Necessary Data

From an intelligent infrastructure perspective, "smart" communities provide opportunities to quickly obtain the big picture in a crisis. Many communities have solutions in place providing near real-time information about the surrounding environment, such as traffic sensors or automated video streams.

Surveying the impact of a disaster is a top priority when managing a response. Drones are a proven method to quickly survey vast areas, but asset coordination and deployment is complex. Data-driven Internet of Things (IoT) applications provide emergency managers with information and management capabilities to plan and coordinate airspace mapping, pilot credentialing, drone registrations and FAA compliance.

Understanding which fleet assets have arrived, where they are staged, or what is in-transit will add to the common operating picture. The ability to map assets in relationship to a moving storm or areas cut off by the disaster contributes to the who, what, where and when of the response.

Security

When disasters strike, cyber adversaries immediately step up attacks. We've all heard cyber statistics, but how do cyber attacks relate to first responders? Examples are prevalent: in 2018, a massive cyber attack hobbled Atlanta's municipal systems, forcing police and rescue personnel back to pen and paper. In 2017, hackers took over 123 of 187 network video recorders used to monitor public safety in an area of Washington, DC. Although just two examples, the impact on mission and life is obvious.

To defend against attacks, public safety agencies must develop a cyber resilience strategy that covers mobile field responders and remotely managed equipment. This strategy should be quick and easy to deploy and scale as resources expand, roles change and personnel enter and exit the scene.

To provide full protection, cybersecurity strategies should address the following three attack vectors:

Secure the Network – Data in transit

Smartphones, tablets, modems, routers and other machine-to-machine (M2M) devices should be considered an extension of your network, whether in the field or in an emergency operations center. Agencies need to safely integrate these devices into existing systems without compromising control and management.

Separating mission-critical data in transit from public traffic via virtual private networks (VPNs) eliminates the risk of unsolicited traffic from external sources. While VPNs protect data in transit over the Internet, removing access to the Internet adds even more protection. Leveraging mobile private networks, data connectivity from cellular devices can be routed directly to agency networks via point to point circuits or Multiprotocol Label Switching (MPLS), or to cloud applications via solutions like Secure Cloud Interconnect. Bypassing the public Internet for specific applications or hardware reduces the potential for a myriad of attacks on the integrity of the data.

Secure the device

Pushed or downloaded management applications can provide visibility into the status of devices and applications in an emergency. Devices can be compromised from trojans, spyware, out-of-date operating systems and configuration risks. Agencies need policy-driven configurations and dynamic monitoring. These provide visibility into devices, apps, networks and the status of operating system firmware, allowing only trusted devices connect to agency infrastructure and data.

Secure the application

Mobile device applications are prime targets for cyber attacks. A single device hack could give attackers enough access to disrupt recovery communications. Monitoring and defending applications during a crisis ensures communications, visibility, situational awareness and access to critical infrastructure.

Products such as Software Defined Perimeter (SDP) provide an "over the top" security solution that can fit any customer environment without requiring a re-architecture of the existing infrastructure or security elements. This cloud driven protection, creates "need-to-know" or "zero-trust" authenticated access between devices and applications. Users get only the apps they need, while bad actors can't attack what they can't see. SDP is a cloud-based and highly scalable managed security solution that builds tunnels between applications and your network to securely connect users to resources.

Connectivity

Communications is a fundamental priority in any disaster response plan. First responders rely on Long-Term Evolution (LTE) networks for mission-critical data, because LTE is the most widely used and inter-operable solution for voice communications.

History has shown that LTE networks are the most reliable and resilient communication paths during a disaster, and LTE is backed by technologies which can be rapidly deployed to extend connectivity even in the worst hit areas. Understanding what resources and technologies are available before a disaster strikes will greatly improve mission outcomes.

LTE is a Lifeline

Some network providers have dedicated disaster response teams who train and deploy with first responders. These teams understand that connectivity is a lifeline for responders and a community in need.

"At Verizon, we have a team called the Business Continuity and Emergency Management (BCEM) group, which is responsible for ensuring our public safety services are resilient and for coordinating our emergency response plans," explained Kent Kildow, director of BCEM at Verizon.

> **"We use the Incident Command Structure as the foundation for how we plan and address disasters and deploy cross-functional teams into the field supporting recovery efforts."**

These recovery efforts feature a large assortment of rapidly deployable network connectivity solutions such as cells on wheels (COWs), cells on light trucks (COLTS), smartphones and tablets with priority services for first responders, along with charging stations and many other services.

As part of an emergency response plan some agencies choose to purchase or lease connectivity solutions for quick deployment, especially in low coverage areas. These include LTE deployable communications trailers, which can quickly provide cellular coverage to a large number of devices. Or for high impact zones or areas with limited accessibility, network connectivity may be best extended through small, portable and secure LTE solutions that are easy to use and available in backpacks or hard-shell cases.

Mobility

Mobility has proven itself as the basic building block of modern communications and the advancement of first responder capabilities. Mobility enables situational awareness, field coordination, and communications. Capturing real-time events, streaming video or data, and deploying resources based on informed communications can save lives.

Data is critical, but people are the biggest part of any disaster response. Resource orchestration relies on the ability to effectively communicate and share data with mobile resources on the ground. Advancements in the network and connected devices have supported the evolution of public safety capabilities.

> **"Mobility is much more than the typical smartphone most of us think about,"says Nick Nilan, Director of Public Sector Product Development at Verizon.**

"You need access to applications such as navigation, and ideally offer the accessories first responders have become accustomed to with Land Mobile Radio (LMR) devices – external microphone with clip, hardened case or device itself. As agencies transition from LMR to LTE they're looking for LMR familiar capabilities with more interactive and informational functions."

Smart applications available via download and solutions such as push-to-talk have increased collaboration and situational awareness. Newer devices are designed to support extreme environments and smart applications. Just as mobile apps provide so much day-to-day convenience for people during normal times, apps are being outfitted for duty in a crisis.

Outfitting first responder vehicles with wireless routers provides a secure LTE broadband connection for the transfer of real-time information and vehicle tracking. The embedded WiFi hotspot feature extends broadband capabilities to multiple devices such as laptops, video recorders, body cameras and medical equipment.

Mobile IoT devices are becoming more relevant and versatile in a response. Although most people are familiar with drones, small IoT devices the size and shape of a softball can equally support responders. These devices can provide 360-degree streaming video in high-risk situations with the ability to throw, tether, or role into tight spaces or compromised structures.

The Network

First responders rely on highly flexible, scalable and efficient network infrastructure to provide the highest priority emergency communications. There has been much coverage recently of terms like private core, preemption and priority communications, but confusion persists regarding what these terms mean and how they impact the service delivered.

“We offer priority and preemption service free of charge to qualified first responders, and we’re going beyond those solutions to further extend their LMR networks,” says Steve Miller, National Security Lead for Verizon Enterprise Solutions, and a former Illinois state trooper. “We offer the ability to bridge their LMR networks to the Verizon national LTE footprint along with a range of purpose built services for first responders today and a roadmap of cutting edge solutions for tomorrow.”

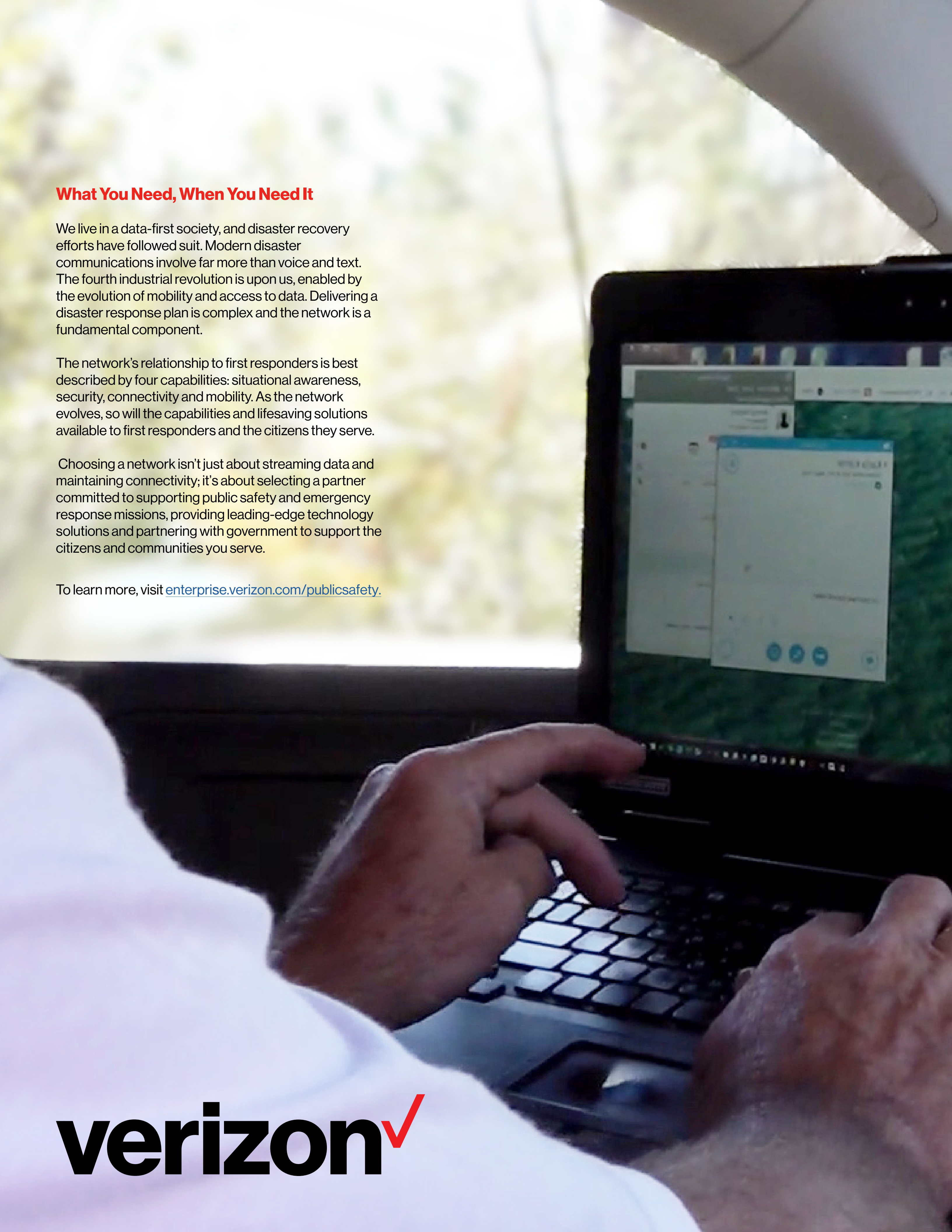
It’s important to understand that there are no government policies or mandates forcing first responders to choose one network provider vs another. Choice is important in making sure the solution is right for each organization. There is more than one dedicated private core for public safety communications, and agencies can choose which provider will give the coverage and reliability they need.

Important Terms

Public safety private core:
A set of gateways and routers specifically prioritized and dedicated to segmenting and processing public safety data

Preemption:
The ability to segment additional bandwidth (more data traffic pipes) from the commercial/consumer network if the public safety private core ever experienced congestion

Priority:
First responders would have higher priority connecting to cell towers and the network than commercial or consumer users



What You Need, When You Need It

We live in a data-first society, and disaster recovery efforts have followed suit. Modern disaster communications involve far more than voice and text. The fourth industrial revolution is upon us, enabled by the evolution of mobility and access to data. Delivering a disaster response plan is complex and the network is a fundamental component.

The network's relationship to first responders is best described by four capabilities: situational awareness, security, connectivity and mobility. As the network evolves, so will the capabilities and lifesaving solutions available to first responders and the citizens they serve.

Choosing a network isn't just about streaming data and maintaining connectivity; it's about selecting a partner committed to supporting public safety and emergency response missions, providing leading-edge technology solutions and partnering with government to support the citizens and communities you serve.

To learn more, visit enterprise.verizon.com/publicsafety.

verizon✓