At-A-Glance

Maintaining Government Services Under Extraordinary Circumstances

Five Steps to Achieve and Maintain Continuity

Uninterrupted delivery of services requires thorough integration of networking and communications technologies across the organization. This is especially true when disaster strikes. Appropriate and effective responsiveness requires planning and collaboration.

Government agencies need to protect vital information, establish contingencies that allow staff to perform functions under extreme conditions, and maintain access to critical resources among agencies and citizens through interoperable communications.

Cisco's Five-Step Approach to Continuity of Government Helps Protect People and Assets

1. **Prepare:** Adopt early-warning tools and continuity and situation-response plans.
2. **Prevent:** Work to safeguard employees, citizens, property, and data/service information.
3. **Detect:** Provide instant notification of security breaches, disruptions, and threats.
4. **Assess:** Determine the scope of the incident and next actions.
5. **Respond:** Coordinate real-time communication and delivery of critical services.

Collaborative and Integrated Disaster Preparedness

For government agencies, the impact of a disaster can result in suspended services and loss of access to data, applications, and work facilities. Every disaster brings a wave of chaos; only those agencies that are best prepared can respond quickly and effectively to bring disparate elements together and re-establish order to keep critical functions online. Government agencies with disaster recovery plans in place will fare better with greater continuity of services.

To confront contemporary threats and risks, successful strategies focus on collaboration. Integrating all the solution components is essential. People, processes, training, and planning are all part of effective disaster preparedness.

Consider these five key steps when implementing a program for your government agency:

1. Prepare

Create a disaster recovery plan.

A formal plan should be initiated and endorsed by senior management and should involve all levels of personnel in your agency. An inclusive process of gathering information and drafting the plan will create the necessary sense of everyone's ownership in and responsibility for disaster recovery. As you begin your preparations, be sure to include data and application redundancy. This back up is critical to uninterrupted service provision. Specific plans may be tailored to align with each agency's needs, but common elements include:

- Risk and threat analysis
- Leadership and succession plan
- Emergency response plan
- Internal and external communications requirements
- Human resources responsibilities
- Facilities management
- Availability of information and communications technology
- Cooperation with first responders, public officials, vendors, partners, and customers

Create a workforce continuity plan.

If employees can't get to their offices for days, weeks, or longer, it is important to understand what kinds of remote access solutions they need to continue being productive, based on their individual job requirements. For example:

- Back-office workers need access to applications and data in order to utilize email or other collaborative tools to communicate.
- Other categories of employees whose jobs require extensive collaboration may need high-availability voice-over-IP (VoIP) services along with access to corporate data and applications. The benefit of IP and Ethernet in a disaster is that they are so pervasive compared to other technologies that devices are truly "plug and play."

Maintaining Government Services Under Extraordinary Circumstances

All personnel who interact with constituents, partners, or the press may need remote communications solutions with guaranteed quality of service (QoS), a VoIP phone with guaranteed toll-quality service, and collaborative software applications such as Cisco WebEx™ conferencing, which allows audio and video conferencing.

2. Prevent

Understand what data and systems are critical to service continuity.
Many governments have mandated the remote replication and storage of financial, medical, and certain other kinds of data. Data and applications are critical to uninterrupted service provision. Make sure you know where all of your agency's critical data and applications are located and how they can be integrated into a remote backup solution.

Train your staff on disaster response.
Training and practicing facilities evacuation and other emergency responsibilities for certain types of disasters relevant to your agency operations could have dramatic consequences related to personnel safety, service continuity, data confidentiality, and asset security in the event of a real disaster.

3. Detect

Identify and fix single points of failure in your network, processes, and people.
In network design, redundancy eliminates the risks inherent to single points of failure. Make sure that network elements—including switches, routers, and other components—are redundant and enabled with software failover features. Review agency processes and job responsibilities to ensure that there is similar failover, should a process or employee become adversely affected in a disaster.

4. Assess

Determine the scope of the incident and the next actions. These actions and key decision makers should be clearly identified in your plans created under the Prepare step.

5. Respond

Coordinate real-time communication. Train people and put key solutions in place to enable an integrated and immediate communications response during any disruption.

Cisco Helps Prevent Service Disruptions—Even if a Disaster Occurs

Emergencies and disasters often cause disruptions in the services provided by government agencies, communities, schools, and colleges. In some cases, critical services can be disrupted for many days.

For more than 20 years, Cisco® technologies and convergence expertise have helped state and local government agencies maintain operability of their systems, personnel, and applications – often in the midst of extraordinary circumstances New collaboration technologies make it possible for these groups to transform themselves into collaboration-based entities, so they can problem-solve like never before.

Cisco can help with solutions to maintain continuity of government services even when an emergency-related or disaster-related disruption occurs. Whether you are preparing in advance of an emergency or a need arises during an emergent situation, Cisco Capital℠ offers a financing program to help government agencies bridge budget gaps and implement critical solutions immediately.

For example, Cisco solutions helped the Missouri State Highway Patrol support its citizens during a major ice storm that cut power and supplies to the entire southeast part of the state. Installing integrated communications solutions in Emergency Response Vehicles provided situational awareness, helped teams to communicate across jurisdictions, and brought help to citizens faster.

Why Cisco?

- Cisco provides intelligent, secure, resilient network infrastructure with the mobility necessary in a time of crisis.
- Cisco is a leader in unified communications, a core solution that uses the network as the platform to maintain critical continuity in the event of a disaster.
- Cisco has a proven record in introducing technologies in the safety and security market that easily integrate with Cisco network architecture.
- Cisco collaborates with safety and security technology partners to meet your requirements for a converged network solution.

Cisco End-to-End Network Provides Continuous Availability
Incorporating advanced foundational networking, communications, mobility, and security, Cisco aligns technology with progressive processes to provide state and local governments with new capabilities for facilitating service effectiveness, citizen empowerment, public safety and security, social inclusion, and economic development.

Learn More
To learn more about continuity of government, visit: **www.cisco.com/go/govcontinuity**.