

PLANNING IS THE  
KEY TO SUCCESSFUL  
DISASTER  
RECOVERY



Source: *US State Government Disaster Recovery Markets* by Frost & Sullivan, A Global Growth Consulting Company

## DISASTER PLANNING AND RECOVERY

In the aftermath of Hurricane Katrina, local and state government services and systems were strained severely by a combination of factors. Damage to critical infrastructure was widespread in the affected areas. Communications between state and local government agencies was interrupted. Emergency services communications were disrupted, delaying the delivery of services to affected areas. No type of communications infrastructure was protected from the storm. Wireless network towers, telephone poles, central offices, and Public Safety Answering Points were knocked out of service. Primary and backup power sources were equally affected and impaired. Broadcast systems, including cable television, broadcast television, and broadcast radio were also severely damaged.

But the greatest damage was in human terms. From loss of life to loss of confidence, the damage to communities, families, and institutions was immeasurable.

The Federal Communications Commission reported Hurricane Katrina knocked out more than 3 million customer phone lines in the Louisiana, Mississippi, and Alabama area.

- more than a thousand cell sites were out of service
- as many as 700,00 cable television lines were out of service
- millions of telephone calls were incomplete
- 37 broadcast radio stations in the area were disabled
- 20 telephone switching centers were out of service
- approximately 1,700 DS-3 interoffice facilities were out of service
- six public safety answering points (PSAPS) were out of service
- approximately 100 radio and television stations off the air.
- communications sites were dependent on back-up power

The 2005 hurricane season was a watershed event for the information age. There simply had not been a single natural disaster of this magnitude since the advent of the internet economy and the subsequent introduction of the eGovernment era.

Perhaps for the first time, state and local governments, along with private business and the public, understand their shared urgent vulnerabilities to disasters and the crucial importance of a comprehensive disaster recovery plan to protect communications networks. The aftermath of Hurricane Katrina cut aid workers and first responders off from their organizations and their constituents. The crisis underscored the need for local and state governments to secure their communications infrastructure, build in redundant systems, and educate their constituents on the importance of being self-sufficient in the event of future disasters.

---

“The greatest damage was in human terms. From loss of life to loss of confidence, the damage to communities, families, and institutions was immeasurable.”

---

---

“The crisis underscored the need for local and state governments to secure their communications infrastructure, build in redundant systems, and educate their constituents on the importance of being self-sufficient in the event of future disasters.”

---

## PLANNING IS THE KEY TO SUCCESSFUL DISASTER RECOVERY

Natural disasters cannot be prevented, but the effects of a disaster can be mitigated by careful planning and through public and private partnerships that take advantage of existing resources. Just as state and local governments take responsibility for maintaining public safety; key business sectors take responsibility for providing critical information and communications services. Healthcare, energy, housing, transportation, and food distribution services are all essential parts of an orderly recovery from disaster.

## SELECTION OF HARDENED ASSETS

A key lesson from the 2005 hurricane season is the importance of being selective. Governments, businesses, and citizens must all be very selective when choosing systems, services, and products. From flood control architecture to family first aid and survival kits, the decisions are all-important in the event of a disaster. The same decisions must be made when selecting critical information and communications technologies with the goal of surviving a disaster.

Citizens, businesses, and governments must be prepared to continue operation and to secure themselves during a disaster. Access to power, water, food, shelter, money, and medical care can be limited during a catastrophic event. The goal should be to ensure an orderly response through a resilient communications network. Information and communications are essential to the effective distribution of resources. When communications and information networks fail, the recovery process is delayed and the potential of a ripple effect is much greater.

State and local governments can choose from a wide range of wireline and wireless communications networks. Choosing a technology, a system integrator, or a network partner requires defining the business continuity requirements and the service level agreements for each service in the network and in the data center. For example, first responder communications may be considered the most mission-critical service supported by the network. An SLA for first responder communications would have more resources associated with it than the SLAs of other less important services.

If network links between public safety answering points, police, communities, hospitals, and paramedical teams are paramount, then the appropriate selection processes must be applied to ensure that the network has built-in redundancy and survivability.

---

“Natural disasters cannot be prevented, but the effects of a disaster can be mitigated by careful planning and through public and private partnerships that take advantage of existing resources.”

---

---

“A key lesson from the 2005 hurricane season is the importance of being selective. Governments, businesses, and citizens must all be very selective when choosing systems, services, and products.”

---

While designing a disaster recovery strategy, it is tempting to provide full backup of every service, every circuit, and every server and system in the environment. However, the objective is to successfully restore the environment after an outage or disaster, and should focus on the following goals:

- Communications services and resources should be easy to access and widely available.
- Restoration of service should be as quick as possible.

These two goals can be achieved by defining disaster recovery objectives.

*Recovery Point Objective (RPO)*: The point in time to which systems and data must be recovered after an outage (e.g. end of previous day's processing). RPO's are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered.

*Recovery Time Objective (RTO)*: The period of time within which systems, applications or functions must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

A detailed analysis of business requirements and defined mutually acceptable SLAs for each service is followed by exploring of the technical aspects of the backup and recovery solution. The key factors to be considered here are the different backup modes, types, topology, and factors that you must take into account when you design backup and recovery solutions

## **THE ROLE OF NETWORK PROFESSIONAL SERVICES IN DISASTER RECOVERY PLANNING**

Professional Services needed to manage effective disaster recovery planning include consulting, design, implementation, and maintenance of agencies' communications infrastructure. The disaster recovery function can be an outsourced function provided by a managed telecommunications service provider using existing infrastructure and hardened assets. Disaster recovery and business continuity are high profile responsibilities for state and local governments. Failure can be disastrous on both a human and political level. The drivers for recovery and continuity are government's responsibility to provide the public with reliable emergency services. This responsibility is fundamental to comply with homeland security initiatives. Hurricane Katrina caused a regional disaster with intensive local and national effects. This fact is now forcing state and local governments to coordinate more rigorous contingency planning. The impact of the hurricane season on critical infrastructure further complicated the need to monitor, protect, identify and prioritize data points on people, places and things. The storage, retrieval, and transmission of this critical data on community infrastructure, utilities, and populations are an essential challenge among both local and state agencies. In an emergency, it is essential to identify threats and resources, whether these are people, facilities, or vehicles. The value of the

---

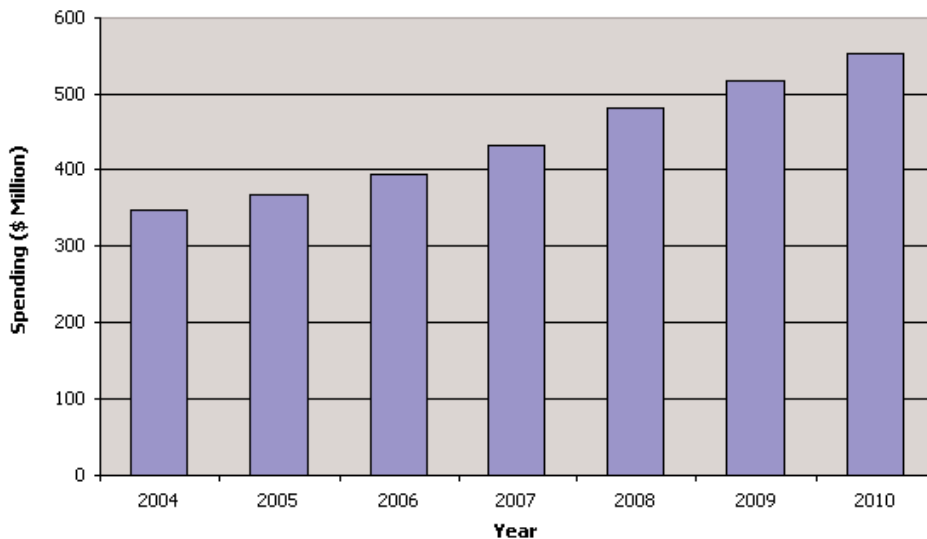
“Disaster recovery and business continuity are high profile responsibilities for state and local governments. Failure can be disastrous on both a human and political level.”

---

information can turn the tide in a disaster, but can only be used if the communications network survives. These complexities drive the need for skilled IT personnel in key advisory roles and in the ranks of selected partners. The need to manage communications networks and information assets is key to a successful disaster recovery solution.

Frost & Sullivan forecasted government and business spending on disaster recovery to grow dramatically. The pressures caused by post-Katrina recovery have continued to focus attention on the need for more budget dollars and more efficient execution.

State Government Disaster Recovery Market:  
Total Telecommunications Spending Forecasts (U.S.), 2004-2010



## DISASTER RECOVERY RESOURCES

Disaster Recovery can be defined as the ability of a business, a family, or a government agency to resume normal operations after a catastrophe. A disaster contingency plan includes backup systems, supplies and services for essential communications and information processing. A recovery plan includes immediate actions and long term measures for responding to emergencies caused by natural disasters, accidents, or attacks. The resources identified in the contingency plan are essential to business continuity in the immediate aftermath and in the period that follows a disaster. It is not sufficient to identify critical weaknesses without taking the appropriate actions to back-up those systems in an emergency.

The process of developing a plan involves all parts of an organization, identification of critical resources and basing the plan for recovery on how long the organization can function without specific resources. For example, a local government may decide that it cannot provide emergency services if the public safety answering point fails for longer than eight hours. The contingency plan must be updated continuously to address potential risks. A disaster may make normal functions impossible, and requires redundant systems,

networks, and sites to minimize interruptions and insure the organization will be able to resume mission-critical functions.

There is no single definition for a technology related disaster. In disaster recovery, consequences drive action, with business resumption activities taking center stage. The primary goal is the restoration of critical business operations and systems access. The potential forms of disasters that could adversely impact state and local government agencies' communications infrastructure include:

- Hardware and software failure resulting in data loss
- Corruption of data due to power failure
- Network failure
- Virus attacks resulting in data corruption or data loss
- Physical damage from fire, flood, earthquake, or wind
- Criminal or terrorist destruction of critical infrastructure

Disaster recovery planning analyzes business processes and continuity needs; it should also include a major focus on prevention measures.

## **SUGGESTED DISASTER RECOVERY PLANNING PHASES:**

### Phase I

Business Impact Assessment (BIA) is the process for determining the acceptable level of impact to a government agency business process and function. This phase focuses on the impact to the public resulting from the loss of agency processes and functions.

### Phase II

Strategy Development is the process for identifying detailed resource requirements, developing alternatives for recovery, and selecting a cost-effective strategy based on the Business Impact Assessment conducted in Phase I.

### Phase III

Strategy Implementation is the process for implementing the strategy that was selected during the Strategy Development Phase.

The risk of telecommunications service outage is a crucial part of disaster recovery planning. This concern intensified due to increasing threats from natural causes, terrorism and hacking. Because IT infrastructure depends on the telecommunications network, the planning process must address network services. Voice and data networks interconnecting government agencies play an important role in disaster recovery planning. It is essential

---

“There is no single definition for a technology related disaster...The primary goal is the restoration of critical business operations and systems access. ”

---

---

“It is essential to have a redundant network in place to maintain voice and data communications during network failure or where fail over to an offsite location is required.”

---

to have a redundant network in place to maintain voice and data communications during network failure or where fail over to an offsite location is required. Telecom networks are critical to providing the link for remote replication of data and offsite data storage.

Telecommunication links between government agencies and the public are critical. Both wireline and wireless infrastructure are vulnerable to catastrophic disasters. Disruption of telecom service is intolerable because it is the lifeline to emergency services from fire, police, and emergency medical personnel. Frost & Sullivan recommends that every major telecom project issued by state or local government must include network disaster recovery planning for business continuity. Spending on telecommunication & IT for public safety, emergency notification and first responder functions are essential responsibilities of state and local government.

## **INCREASING FOCUS ON CRITICAL INFRASTRUCTURE PROTECTION**

Critical infrastructure assets have been defined as physical and logical assets so vital that disruption, infiltration, incapacitation, destruction or misuse will have a debilitating impact on the health, safety, welfare or economic security of citizens and businesses. Critical Infrastructures includes people, facilities, physical networks, and information assets.

Recent events have triggered a heightened need to safeguard critical infrastructure from disaster. Physical security precautions include designing structures that can withstand hurricane force winds and flooding. The networks that support critical facilities must be protected to support electronic security monitoring, access control, intrusion detection, non-intrusive inspection, sensors, explosive detection and environmental controls.

## **PUBLIC CONFIDENCE AND PUBLIC SAFETY**

The greatest benefit of effective disaster recovery planning is the maintenance of public trust, safety, and confidence. Perhaps the most essential role of government is to ensure the welfare of the public in times of dire need. Disasters strain government resources and can erode public confidence. Public trust can be maintained throughout a disaster by resilient communications, broadcasting, and information services. A rapid coordinated response to disasters is the most effective way to protect life and property and to preserve the fabric of local communities.

---

“The greatest benefit of effective disaster recovery planning is the maintenance of public trust, safety, and confidence.”

---

## CONTACT US

**Bangalore**

**Bangkok**

**Beijing**

**Buenos Aires**

**Cape Town**

**Chennai**

**Delhi**

**Dubai**

**Frankfurt**

**Kuala Lumpur**

**London**

**Mexico City**

**Mumbai**

**New York**

**Oxford**

**Palo Alto**

**Paris**

**San Antonio**

**Sao Paulo**

**Seoul**

**Shanghai**

**Singapore**

**Sydney**

**Tokyo**

**Toronto**

**Silicon Valley**  
2400 Geng Road, Suite 201  
Palo Alto, CA 94303  
Tel 650.475.4500  
Fax 650.475.1570

**San Antonio**  
7550 West Interstate 10, Suite 400,  
San Antonio, Texas 78229-5616  
Tel 210.348.1000  
Fax 210.348.1003

**London**  
4, Grosvenor Gardens,  
London SW1W 0DH, UK  
Tel 44(0)20 7730 3438  
Fax 44(0)20 7730 3343

**877.GoFrost**  
[myfrost@frost.com](mailto:myfrost@frost.com)  
<http://www.frost.com>

### ABOUT FROST & SULLIVAN

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies, and the investment community, by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics, and demographics. For more information, visit <http://www.frost.com>.