America's Broadcasters: Your First Informers

10 STEPS TO DISASTER PREPARATION AND RECOVERY

Television and radio stations play a unique role as first informers during disasters, providing breaking news alerts and round-the-clock reporting to keep their communities safe before, during and after emergencies. Given the resiliency of the broadcast infrastructure, broadcasting is often the only communications outlet available during disasters, especially when cell service or the internet go down. Thus, it is critical that broadcasters plan ahead to safeguard their facilities and staff in case of an emergency. The ten steps below serve as a general guide to help broadcasters stay on the air during disasters.

STEP 1 ▶ PREPARE A DISASTER RECOVERY PLAN

Convene a cross-section of staff to work on a plan. Broad participation produces the most useful plans.

- ☑ Station engineers: Identify operational and technical risks
- ☑ General managers: Oversee staff safety, training and communications
- ☑ News directors, producers and reporters: Plan for continuous news coverage and remotes
- ☑ Station owners: Champion a commitment to disaster planning

The plan must address certain factors and consider both natural and man-made disasters.

- ☑ Identify and assess risks
- ☑ External and internal communications
- ☑ Mitigation strategies
- ☑ Emergency supplies
- ☑ Critical equipment, systems and services
- ☑ Staff training and safety
- ☑ Provide emergency news to all segments of your audience
- ☑ Distribute, periodically review and test the plan
- ☑ Staff roles and duties

STEP 2 ▶ REVIEW YOUR RISKS

What are the most likely natural disasters that could impact your station?

- ☑ Are you in a flood zone?
- ☑ Stations on the West Coast should secure their facilities and equipment in case of an earthquake or possible wildfires
- ☑ Research the high-water marks in your area
- ☑ If hurricanes or tornados are common, prepare your facility for high winds and extreme rain
- ☑ Freezes and icing can impact the Southeast, and major snowfalls affect the North. All stations should check for nearby tall trees or rock formations that could cause damage

What kinds of man-made emergencies could affect your operation?

- ☑ Make sure there are no buried pipelines or exposed gas meters that could pose a danger
- ☑ Prepare for power outages and need for fuel
- ☑ Assess your risks for equipment failure
- ☑ Find out if hazardous materials are housed or transported nearby
- ☑ Consider your vulnerability to a pandemic
- ☑ Identify the potential for terrorist or cybersecurity attack

What needs to be protected?

People: Your staff is a station's most important asset. Make a plan that keeps your staff and their families safe during emergencies

Facility: Review the security, reliability and redundancy of your tower, antenna, transmitter, microwave and studio-transmitter links (STL) and any other system needed to stay on the air

Supply chain: Make sure your station is prepared for power failures and equipment breakdowns

News delivery: Plan for alternative methods of reporting and distributing programming

STEP 3 ▶ ENGAGE STATION LEADERSHIP

Ownership and management set the priorities of a station. Their commitment lets staff know that devoting time and money to disaster planning is important. Leadership can also provide a holistic view of a station's many functions and identify connections among departments that may be vulnerable. Station leadership can also address other important risks like damage to a station's image or reputation.

Station leadership and management should use "sunny days" to engage with federal and local government officials, public safety authorities and emergency managers to cement relationships that could be critical during emergencies for purposes of news reporting and access to facilities.

STEP 4 ▶ EXPECT THE UNEXPECTED

The studio must be evacuated. Can you broadcast from another location? How will you get there? How long will it take to restart operations? Can you originate programming from there?

Focus on single points of failure that could knock your station off the air.

- ☑ Do you have a backup tower or auxiliary transmitter or another way to broadcast?

- ☑ Microwave, fiber or STL links are lost. Can you receive or deliver content another way?

- ☑ Phone or internet access go down. Do you have a plan for communicating with staff, local public safety and clients, such as with a satellite phone or internet system?

- ☑ Electricity is lost or equipment breaks. Do you have a backup generator and a fuel contract to keep it running, for both the studio and transmitter? Have you made arrangements with vendors and contract engineers for a first right to obtain goods or services?

- ☑ Are your equipment and facilities secure from unauthorized access in case you have to evacuate?

- ☑ Do you have plan in case of a cybersecurity disruption, or your computer system or server is corrupted?

STEP 5 ▶ PROGRAMMING CONTINUITY

Broadcasting is never more important than during an emergency. Make sure you can deliver the news even if your station goes down. Have a plan in place to carry programming from a network or other local station, or simulcast on another station.

Pre-arrange plans to provide news over another local station, or to stream programming online during an emergency, especially foreign language stations that may provide the only news in a particular language in an area.

- ☑ Create protocols for issuing EAS alerts

- ☑ Have a plan for continuous closed captioning service

STEP 6 ▶ SIMPLE FIXES CAN MAKE A BIG DIFFERENCE

Don't forget about common sense measures that can prevent or minimize problems.

- ☑ Use glass with a high safety rating in windows and doors

- ☑ Tether equipment racks securely and use safety chains to secure heavy objects

- ☑ Anchor computer monitors to desktops

- ☑ Bolt critical workstations to the floor or walls

- ☑ Keep cars and remote equipment in multiple locations

- ☑ Secure your facility: surveillance cameras, door entry keys and locks, fencing, perimeter security and reception security

- ☑ Maintain backup data and records off-site

- ☑ Schedule routine maintenance of all systems and equipment

STEP 7 ▶ STAFF SAFETY AND COMMUNICATIONS

Identify and mark locations in facility for shelter-in-place.

- ☑ Store essential supplies: food, water, batteries, bedding, battery-powered radio, National Oceanic and Atmospheric Administration radio, flashlights, first aid kid, dust and filter masks, sanitation needs, tools, plastic sheeting and duct tape. Make sure at least one employee is trained in first aid

- ☑ Encourage staff to keep a "go kit" at work for clothing, medications and toiletries In case of evacuation, make a plan for communication with staff, including a process for checking in and equipment like two-way radios or satellite phones. Keep contact information on hand for local public safety and emergency management agencies, as well as clients and vendors

- ☑ Keep important documents in a portable waterproof, fireproof safe, including building plans, insurance policies, employee information and bank account records

STEP 8 ▶ TRAINING, TESTING AND POST-DISASTER REVIEW

Periodically train your staff on the disaster recovery plan. Use a quiz or other exercise designed to make sure everyone knows their role.

Certain staff may be unavailable when disaster strikes, so cross-training is essential:

- ☑ Train back office staff and management for on-air and production operations like call screening, board operations, field producing, reporting and emergency announcement processing

- ☑ Train board operators to make simple technical repairs

- ☑ Make sure multiple employees know how to process EAS messages

Drill your staff on putting the plan into action. Test various scenarios:

- ☑ Loss of master control operations

- ☑ Switch to newsroom or production studio

- ☑ Test production from alternative location or transmitter

- ☑ Imminent threat to station facility

- ☑ Evacuation and meet-up site
- ☑ Move operations to another site or remote vehicle
- ☑ Maintain communications among staff
- ☑ Safe shelter-in-place location
- ☑ Transmitter failure
- ☑ Switch to backup antenna
- ☑ Simulcast on another station

Following an emergency, conduct a thorough debriefing with staff to identify any lessons learned and improve preparedness for future events.

Review the success of remote operations, access to fuel, communications, partnerships with other stations, and most important, the safety of staff, to assess whether any changes to your emergency preparedness plan are needed.

STEP 9 ▶ CYBERSECURITY PREPAREDNESS

Cyber attacks and disruptions have become a more frequent concern. At a minimum, stations should implement basic cybersecurity hygiene best practices designed to mitigate cyber risks:

- ☑ Security barriers such as hardware, software, network and cloud firewalls
- ☑ Strong password security and multi-factor authentication
- ☑ Secure Wi-Fi
- ☑ Secure data storage and backups
- ☑ Install and regularly updated antivirus software
- ☑ Regular updates of operating system and applications
- ☑ Staff training against phishing and other cyber threats

More resources can be found at:

- ▪ **Federal Communications Commission:** https://www.fcc.gov/sites/default/files/cyberplanner.pdf
- ▪ **Cybersecurity & Infrastructure Security Agency:** https://www.cisa.gov/topics/cybersecurity-best-practices
- ▪ **National Institute of Standards and Technology:** https://www.nist.gov/cyberframework

STEP 10 ▶ INSURANCE

- ☑ Explore the various kinds of insurance that may help you recover from a disaster
- ☑ Property insurance may compensate for building damage, internal water damage, electrical malfunctions and theft
- ☑ Flood insurance availability may depend on your location. Internal flooding caused by broken pipes, leaking roofs and accidental spills is likely covered by property insurance. Loss of income or business interruption insurance may cover temporary needs like renting equipment to continue broadcasting and security personnel
- ☑ Marine insurance is used to underwrite broadcast equipment like towers, transmission lines, transmitters, STLs and remote equipment
- ☑ Cybersecurity insurance can help cover losses related to cyber disruptions of service