Continuity of Broadcast Operations
Every Station Should Have a Plan

Manny Centeno, Program Manager
DHS, Federal Emergency Management Agency – NCP, IPAWS
Washington, DC

Abstract - *How quickly a broadcast station can return to the air after a terrorist attack, tornado, hurricane, fire or flood often depends on emergency planning done today. The lessons of Hurricane Katrina, Hurricane Sandy, the 1993 World Trade Center bombing, the 1995 Oklahoma City bombing and the September 11, 2001 terrorist attacks demonstrate the importance of being prepared. When it is also considered that the number of declared major disasters nearly doubled in the 1990's compared to the previous decade, preparedness becomes an even more critical issue. Though each situation is unique, any station can be better prepared if it plans carefully, puts emergency procedures in place, and practices for all kinds of emergencies*

Introduction

This paper presents a framework and best-practices for developing a solid Continuity of Broadcast Operations (COBO) Plan for your company, cluster or single station to be prepared for major disasters.

Mass media plays a critical role both in the pre-disaster preparation and warning phase, as well as during and after the emergency. However, at times, broadcasters are directly affected by these disasters.

You should plan in advance to manage any emergency. Be prepared to assess the situation, use common sense and available resources to take care of yourself, your co-workers and your station's operation.

Risk & Vulnerability Assessment

The field of Risk Assessment can be a sophisticated area of expertise that ranges from self-assessment to an extensive engineering study. The size and scope of your individual station will determine your risk assessment needs and the complexity of the assessment. However, you should find out which disasters are most common in the areas where you operate and keep your assessment and resulting plans simple, easy to exercise and execute when needed. Assessing your station's risk and vulnerabilities provides you with the information you need to craft a plan that allows you to harden your physical plant and operation for broadcast continuity.

You may be aware of some of the risks that may affect your stations; others may surprise you. These may include natural emergencies, such as tornadoes, flooding, snowstorms, urban fires or wildfires, hurricanes, tsunamis, earthquakes, gas leaks, food and water contamination, transmitted diseases and pandemics and other risks. You should also be aware that biological, chemical, explosive, nuclear or radiological attacks may pose a threat to your broadcast operation and the community you serve.

Continuity Planning

Carefully assess how your company functions, both internally and externally, to determine which staff, locations materials, procedures and equipment are absolutely necessary to stay on the air. Start by reviewing your on-air process to identify operations critical to survival and recovery. Ask yourself these questions:

- If this studio or building must be evacuated or is unfit for use, where do you operate from to originate live and local programming?
- If power to studio or transmitter is lost, what is your backup plan?
- If you lose our studio-transmitter link, how do you connect?
- What do you do if our antenna or tower is damaged or lost?
- How do you remain on air if your transmitter or transmission line is damaged and the station is off-air?
- What is the backup plan if telephone systems are down?
- If you lose data connectivity, how do you communicate via email or update the website?
- How do you receive critical news if satellite links are lost?

These are just a few of the questions you should be able to answer if you have even a basic continuity plan. It is very important to establish procedures for succession of engineering and operations. For example, is there someone

in another city or state that can fill in if you or your station staff is unable to respond? Do you have a contract engineer that may be able to assist in extreme circumstances? Does someone from programming or sales have basic technical abilities and can assist?

Continuity planning should include all departments within your station. Decide who should participate in putting together your emergency plan. Include staff from all levels in planning and as active members of the emergency management team. Consider a broad cross-section of people from throughout your organization, but focus on those with expertise vital to basic broadcast functions. These will likely include people with technical skills as well as on-air personnel and managers. Identify key suppliers, resources and other businesses you must interact with on a daily basis. Develop professional relationships with more than one company in case your primary contractor cannot service your needs. This is especially important for suppliers such as generator service companies and fuel delivery. A disaster that shuts down a key supplier can be devastating to your operation.

Your employees and co-workers are your business's most important and valuable asset. Effectively communicating with your staff is central before, during and after a disaster. Work with station management to create and distribute emergency preparedness information in newsletters, on company intranet, periodic employee emails and other internal communications tools. Consider setting up a telephone calling tree, a password-protected page on the company website, an email alert or a call-in voice recording to communicate with employees in an emergency. Designate an out of town phone number where employees can leave an "I'm Okay" message in a catastrophic disaster. Satellite telephones have proved invaluable in times of emergency. Hardware and service costs have dropped considerable over the years making this method of disaster communication much more affordable.

If you have employees with disabilities ask them what assistance, if any, they require. People with disabilities typically know what they will need in an emergency. Ask about communication difficulties, physical limitations, equipment instructions and medication procedures. Identify people willing to help co-workers with disabilities and be sure they are able to handle the job.

Finally, plan what you will do if your building, or studio is not accessible. A backup studio facility in a geographically diverse area from the primary site may assure continued operation during and after a disaster.

Talk with your management, staff, co-workers and frequently review and practice what you intend to do during and after an emergency.

Vulnerability Assessment Critical Questions

- Have you planned for your family in times of emergencies?
  □ Yes □ No
- Have you planned how to keep your pets safe during a disaster?
  □ Yes □ No
- Do you have your staff's contact information readily available?
  □ Yes □ No
- Do you have contact information for first responders, emergency managers, weather services, and others readily available?
  □ Yes □ No
- Do you have your key suppliers' contact information readily available (fuel, generator repair and supplies, critical equipment parts, etc.)?
  □ Yes □ No
- Are your studio or transmitter sites in a flood risk area? Are there any obvious natural hazards that may affect these sites? Has a site assessment been conducted recently? (topographical, structural and natural conditions may have changed over the years due to development and other causes)
  □ Yes □ No
- Are there alternative sites from which to originate local live-programming?
  □ Yes □ No
- Do you have a backup transmitter site?
  □ Yes □ No
- Is there a reliable and operating backup power generator at the studio facilities?
  □ Yes □ No
- Is there a reliable and operating backup power generator at the transmitter facilities?
  □ Yes □ No
- Can the backup power system at the studios and transmitter facilities operate long enough to ensure continued operation? How much fuel is stored at each location and how long can backup power be sustained?
  □ Yes □ No
- Is the backup power switched automatically?
  □ Yes □ No
- Are the backup power capabilities routinely tested under load?
  □ Yes □ No

- Is the backup power system tested while the facilities are disconnected from the power grid to assure proper operation?
  □ Yes □ No

- Is physical security sufficient to prevent unauthorized access to the facilities?
  □ Yes □ No

- If you are not in charge of IT, is your IT staff competent in cyber security?
  □ Yes □ No

- Are strong passwords used throughout the network?
  □ Yes □ No

- Does your IT infrastructure use strong firewalls? Are the firewalls properly configured?
  □ Yes □ No

- Are user passwords made to expire in 90 days or less?
  □ Yes □ No

- Are user privileges revoked when an employee leaves the company?
  □ Yes □ No

- Have you mapped your entire IT network? Do you know what devices or appliances are connected to your network, especially wireless (WiFi) devices (including printers, scanners, audio and video devices)?
  □ Yes □ No

- If national network news agreements do not exist, is there an agreement to carry emergency news from other services?
  □ Yes □ No

- Are there backup signal feeds from the primary satellite downlink or uplink?
  □ Yes □ No

- Can Emergency Alert System ("EAS") alerts be received and rebroadcast from backup facilities?
  □ Yes □ No

- Does the plan include backing up the on-air automation and live-assist and the newsroom computer system?
  □ Yes □ No

Emergency Supplies & Essential Services

When preparing for emergency situations, it's best to think first about the basics of survival: fresh water, food, clean air and warmth. Encourage everyone to have a portable kit customized to meet personal needs, such as essential medications. Talk to your co-workers about what emergency supplies the station can feasibly provide, if any, and which ones individuals should consider keeping on hand.

Recommended emergency supplies include both a battery-powered commercial radio and a NOAA weather radio with an alert function. Include extra batteries, a flashlight, water, food, First Aid kit, whistle to signal for help, dust or filter masks, moist towelettes for sanitation, wrench or pliers to turn off utilities, plastic sheeting and duct tape to "seal the room," and garbage bags and plastic ties for personal sanitation.

Keep copies of important records such as site maps, building plans, schematics, RF settings and proofs, insurance policies, employee contact and identification information, bank account records, supplier and shipping contact lists, computer backups, emergency or law enforcement contact information and other priority documents in a waterproof, fireproof portable container. Store this second set of records at an off-site location.

Planning To Stay or Go

Depending on your circumstances and the nature of the disaster, the first important decision after an incident occurs is whether to shelter-in-place or evacuate. You should understand and plan for both possibilities in advance by developing clear, realistic and well thought out plans. If you are specifically told to evacuate, shelter-in-place or seek medical treatment, do so immediately. Use common sense and available information to determine if there is immediate danger. Assess the condition of your current building and after a complete inspection and review, decide if it is suitable for a shelter-in-place location.

Reach out to other broadcasters in your area and collaborate with them to create cooperative redundancy and geographic diversity. If working with direct competition is undesirable, work with other broadcasters in different services. For example, if you operate a television station contact a radio station to partner with in times of emergency.

Having a backup studio facility, and if possible, a backup transmitter site, is crucial for areas where there are known potential hazards. Such a scenario became a reality in 2005 when Hurricane Katrina struck New Orleans and caused the levees to fail. The station had backup facilities to support such a scenario. Ultimately, WWL in New Orleans was the only radio station on the air during and following the disaster.

Evacuation Plan

Personnel

Some disasters will require employees to leave the workplace quickly. The ability to evacuate workers, customers and visitors effectively can save lives. If feasible, develop a system for knowing who is in your building,

including customers and visitors. Decide in advance who has the authority to order an evacuation. If local officials tell you to evacuate, do so immediately. Identify who will shut down critical operations and lock the doors, if possible. Create a chain of command so that others are authorized to act in case your designated leader is not available.

Locate and make copies of building and site maps with critical utility and emergency routes clearly marked. Identify and label entry-exit points both on the maps and throughout the building. Post maps for quick reference by employees. Plan two ways out of the building from different locations throughout your facility.

You should also establish a warning system including plans to communicate with people who are hearing impaired or have other disabilities and those who do not speak English. Designate an assembly site. Pick one location near your facility and another in the general area in case you have to move farther away.

Try to account for all workers, visitors and customers as people arrive at the assembly site. Determine who is responsible for providing an all-clear or return-to-work notification. Plan to cooperate with local authorities responding in an emergency. If your business operates out of more than one location or has more than one place where people work, establish evacuation procedures for each individual building.

If your station is in a high-rise building, an industrial park, or even a small strip mall, it is important to coordinate and practice with other tenants or businesses to avoid confusion and potential gridlock.

There are some procedures you can put in place before a disaster, but you should also learn about what people need to help them recover after a disaster.

Workplace routines facilitate recovery by providing an opportunity to be active and to restore social contact. Re-establish routines, when possible. Sharing with others can speed personal recovery. Create opportunities for breaks where co-workers can talk openly about their fears and hopes. Offer professional counselors to help co-workers address their fears and anxieties.

Relatives & Pets

It is possible that your staff will need time to ensure the well-being of their family members, but getting back to work is important to the personal recovery of people who have experienced disasters. Encourage adequate food, rest and recreation. Provide for time at home to care for family needs, if necessary. Have an open door policy that facilitates seeking care and family support when needed.

Shelter-In-Place

Determine where you will take shelter during a tornado. Storm cellars or basements provide the best protection. If an underground shelter is not available, go into an interior room or hallway on the lowest floor possible. In a high-rise building, go to a small interior room or hallway on the lowest floor possible. Stay away from windows, doors and outside walls. Go to the center of the room. Stay away from corners because they attract debris. Stay in the shelter location until the danger has passed.

Determine if your studios or transmitter site is in a flood prone area and how flood waters may impact site access.

Inspect your structures to assess how much wind force they can withstand. This will provide you with reasonable expectations in the event your area is affected by windstorms.

If local authorities believe the air is badly contaminated with a chemical, you may be instructed to take shelter and "seal the room." The process used to seal the room is considered a temporary protective measure to create a barrier between your people and potentially contaminated air outside. It is a type of sheltering that requires preplanning. Start by identifying where you will go if you are instructed to "seal the room." If feasible, choose an interior room, such as a break room or conference room, with as few windows and doors as possible. If your station is located on more than one floor or in more than one building, identify multiple shelter locations. Lock doors, close windows, air vents and fireplace dampers. Turn off fans, air conditioning and forced air heating systems. Take your emergency supply kit unless you have reason to believe it has been contaminated. Seal all windows, doors and air vents with plastic sheeting and duct tape. Measure and cut the sheeting in advance to save time.

Finally, be prepared to improvise and use what you have on hand to seal gaps so that you create a barrier between yourself and any contamination.

Fire & Medical

Fire is the most common of all business disasters. Each year fires cause thousands of deaths and injuries and billions of dollars in damage. Have your office, plant or facility inspected for fire safety; ensure compliance with fire codes and regulations. Install smoke alarms, detectors and fire extinguishers in appropriate locations. Put a process in place for alerting the fire department. Plan and practice how people will evacuate in a fire.

Workplace medical emergencies vary greatly depending on the disaster, type of job and the worksite. However, there are steps that can give you the upper hand in responding to a medical emergency. Encourage employees to take basic First Aid and CPR training. If it is feasible, offer on-site classes for your co-workers. You should also keep First Aid supplies in stock and easily accessible. Finally, encourage employees to talk about medical conditions that may require support or special care in an emergency.

Crisis Communications Plan

Detail how your organization plans to communicate with employees, local authorities, customers and others during and after a disaster. Be prepared to provide employees with information on when, if and how to report to work following an emergency. Provide top company executives with all relevant information. It may also be important to update the general public. Inform your customers about whether and when products will be received and services rendered. Tell officials what your company is prepared to do to help in the recovery effort. Also communicate with local, state and federal authorities what emergency assistance is needed for you to continue essential business activity. You should also be prepared to give competing and neighboring companies a prompt briefing on the nature of the emergency so they may be able to assess their own threat levels.

Utility Disruptions

Businesses are often dependent on electricity, gas, telecommunications, sewer and other utilities. Plan ahead for extended disruptions during and after a disaster. Carefully examine which utilities are vital to your business's day-to-day operation. Speak with service providers about potential alternatives and identify back-up options such as generators to power the vital aspects of your business in an emergency.

Backup power generators at studio and transmitter sites have proven invaluable in maintaining broadcast operations when disasters strike. One critical item to keep in mind, in addition to properly sizing the generator and matching load requirements, is assuring that there is sufficient fuel stored on site to maintain operations for a reasonable duration. Of course, duration is determined by load and fuel capacity, however, generator reliability and maintenance are key factors when operating in emergency backup mode.

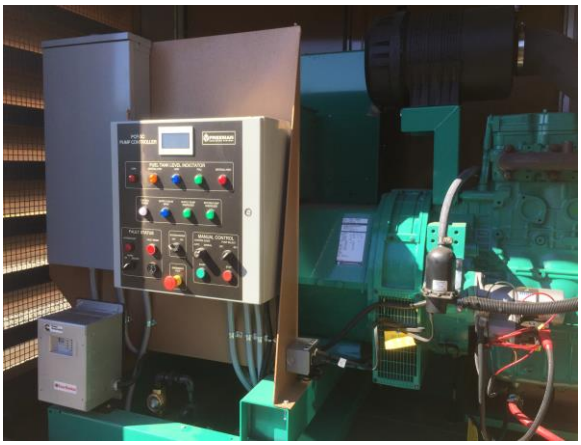

Fig 1 200kW Generator

Fig 2 6,000 Gallon, Double-Walled Fuel Tank

All local, state and Federal environmental laws, regulations and permitting must be adhered to when operating generators and storage tanks. Install and maintain adequate fuel spill prevention measures, monitoring and alerting of fuel leaks. Keep all power generation and fuel storage systems in top shape through active maintenance and exercise.

Fig 3 Fuel Monitoring System

Coordination & Employee Support

Meet with other businesses in your building or industrial complex. Plan to conduct evacuation drills and other emergency exercises together. Talk with first responders, emergency managers, community organizations and utility providers. Plan with your suppliers, shippers and others you regularly do business with.

Just as your business changes over time, so do your preparedness needs. When you hire new employees or when there are changes in how your company functions, you should update your plans and inform your people.

It is possible that your staff will need time to ensure the well-being of their family members, but getting back to work is important to the personal recovery of people who have experienced disasters. Encourage adequate food, rest and recreation. Provide for time at home to care for family

needs, if necessary. Have an open door policy that facilitates seeking care and family support when needed.

Communications

Recent disasters have shown us that communications pathways can be vulnerable to both man-made and natural events. Cellular telephone services may suffer from power disruptions, floods, high winds and congestion. Land lines are similarly vulnerable to these hazards. Mobile communications services are a great convenience on sunny days, but can be life-saving in dire emergencies. Land-line telephone services are essential for day-today business operations. However, in times of disaster are crucial for emergency management and are a vital link to viewers and listeners.

When these "normal" methods of communication fail as a result of a disaster your station not only loses a feedback from your audience, it also loses its ability to request services to maintain operations.

Alternate communications methods and services have become less costly in recent years. Consider partnering with amateur radio operators in your area. They may be able to link critical communications in and out of the station. Additionally, consider satellite communications services. Some services are available on a full-time basis or on-demand. VSAT service is available globally and can be a reasonable solution for your communications needs, including email and other internet services, in an emergency.

Fig 4 VSAT Satellite Antenna

Securing Equipment

The force of some disasters can damage or destroy important equipment. Conduct a room-by-room walk through to determine what needs to be secured. Attach equipment and cabinets to walls or other stable equipment. Elevate equipment off the floor to avoid electrical hazards in the event of flooding. Make an effort to store critical backup equipment at another safe site.

Have your antennas and towers inspected for structural issues. Determine their wind load capacities. Make sure ATUs and other critical equipment is installed high enough to prevent damage water damage. Check for roof leaks and areas where high winds may cause incremental damage.

Building Air Protection

In some emergencies microscopic particles may be released into the air. For example, earthquakes often can release dust and debris, a biological attack may release germs, and a dirty bomb can spread radioactive particles. Many of these things can only hurt you if they get into your body. A building can provide a barrier between contaminated air outside and people inside, but there are ways to improve building air protection.

Building owners or managers, and employers should take a close look at the site's Heating, Ventilating and Air-Conditioning (HVAC) system and be sure it is working properly and is well maintained. Be sure any security measures do not adversely impact air quality or fire safety. Start by developing and practicing shut down procedures. Then, make sure outdoor air intakes are secure. HVAC systems can be an entry point and a means of distributing biological, chemical and radiological threats. Air intakes at or below ground level are most vulnerable because they can be easily accessed. Consider relocating or extending an exposed air intake, but do not permanently seal it.

Finally, determine if you can feasibly upgrade the building's filtration system. Increasing filter efficiency is one of the few things that can be done in advance to consistently protect people inside a building from biological and some other airborne threats. Carefully consider the highest filtration efficiency that will work with a building's HVAC system.

Securing Facilities

While there is no way to predict what will happen or what your business's circumstances will be, there are things you can do in advance to help protect your physical assets. Install fire extinguishers, smoke alarms and detectors in appropriate places. Consider the ways in which people, products, supplies and other things get into and leave your building or facility. Secure ingress and egress. The use of password protected entryways and key fobs has proved very effective for improving physical security. Cameras with a decentralized recording or storage feature are widely used to keep an eye on premises, facilitate identification when intrusions happen, and serve as an effective deterrent.

The nation's battle against terrorism takes place on many fronts, including the mailrooms of U.S. companies. Plan for mail safety.

Broadcast equipment is not always widely available in extreme circumstances. Shipping to and from manufacturers is limited or non-existent in times of disaster. Know your suppliers well and keep their contact information handy.

Cyber Security

Protecting your data and information technology systems may require specialized expertise. However, even the smallest broadcast station can be better prepared. Use anti-virus software and keep it up-to-date. Don't open email from unknown sources. Use hard-to-guess passwords. Protect your computer from Internet intruders by using firewalls. Back up your computer data. Regularly download security protection updates or patches. Make sure your staff know what to do if your computer system becomes infected. Subscribe to the Department of Homeland Security National Cyber Alert System, www.us-cert.gov, to receive free, timely alerts on new threats and learn how to better protect your area of cyberspace.

Here are some basic best-practices you should consider to improve and maintain adequate cyber security at your station:

- Patch your network devices, as necessary.
- Conduct a network Vulnerability Assessment (VA) across your network. VA tools are available online and some are free or open source. These tools can help identify "open doors" which hackers may use to compromise your network.
- VA tools can help identify weak links in your network that, including other devices such as servers, workstations, routers, VOIP servers, etc.
- Establish and understand your perimeter defense. What devices on your network "break" this defense?
- Search for applications that extend through your firewall policies.
- Identify all IP-enabled devices internal to the network.
- Understand if mobile devices are allowed to connect to your network.
- Search for wireless access points that are unknowingly deployed.
- Identify all direct Internet access to and from other devices.
- Use strong passwords on ALL your Internet facing devices. Do not use "dictionary" words for passwords.
- Refresh passwords frequently.
- Discuss your IT security defenses, risks and vulnerabilities with management.
- Disable any unused network access tools or features. For example, if you don't need to access your CAP device via the Internet, shut down the feature; if you are not a public warning originator, disable any features that allow for remote creation of warnings.
- Close any telnet or command prompt services accessible via the web. Consult your manufacturer to know if any "hidden" services or "back doors" need to be patched.
- If practical, isolate your EAS CAP device from other services in your network by creating DMZs and strong firewall protection.
- Ask your manufacturers which ports and services are needed for proper operation of your CAP device.
- Verify that other devices on the same network are not vulnerable to intrusion.
- Although this takes time, look at your network logs regularly to find any obvious intrusion attempts.
- Know your staff… Establish an appropriate credentialing process

Testing

Continual testing is critical to support incremental improvement of broadcast service continuity. Work with your local and state emergency management agencies. Be an active participant in the Emergency Alert System (EAS).

Realistic practice and exercising of your Continuity of Broadcast Operations (COBO) Plan will help you build an effective response when disaster strikes.

References

[1] Federal Emergency Management Agency, "Every Business Should Have a Plan", January 2014

[2] CSRIC, "Local Television Station Model Disaster Recovery Plan & Incident Response Manual", March, 2011