Terrorism *PREPAREDNESS*

The FBI defines terrorism as "the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in the furtherance of political or social objectives".

Terrorism can occur through the use of guns, bombs or arson, but biological, chemical radiological, and computer (cyberterrorism) means can be used. Terrorism preparedness encompasses good crime prevention *plus:*

Generally. . .

- ✶ Be aware of your surroundings - be alert for suspicious activity or packages.
- ✶ Do not touch suspicious packages or items - contact the proper authority.
- ✶ Know where exits are - especially in public assembly areas.
- ✶ Dial 9-1-1 to report emergencies that require police, fire or EMS.
- ✶ Have an emergency kit in your home and car. An emergency kit can help you with man-made emergencies (like power failures or terrorism) or natural disasters (like floods or storms). An emergency kit can include (at a minimum):
  - First aid supplies
  - Flashlight with extra batteries
  - Non-perishable food
  - Drinking water
  - Blanket(s) or sleeping bag(s)
  - Rain gear or a change of clothing

Weapons of Mass Destruction & CBRNE

Weapons of Mass Destruction or WMD are meant to terrorize a population by inflicting many casualties or deaths. WMD can fall into one of five categories represented by the acronym CBRNE.

C - Chemical
B - Biological
R - Radiological
N -Nuclear
E - Explosive

Although the threats of varying hazards are real - conventional explosives will continue to be the method of choice for terrorists.

For the Computer System. . .

- ⇛ All accounts should have passwords that are difficult to guess. Change passwords frequently.
- ⇛ Audit systems and check logs to help in detecting and tracing an intruder.
- ⇛ If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble.
- ⇛ Change the network configuration when defects become known.

Personally . . .

- Don't discuss personal matters such as travel plans, your job, or your family with people you don't know.
- Vary your route to and from work, and the time you arrive and depart.
- Avoid routines (time & location) for shopping, lunch, etc. . .
- Become familiar with the environment. You must know what is normal to be able to detect what is unusual.
- Avoid public disputes or confrontations.

Contingency Planning

Emergency contingency plans should include:

- ✓ Procedure for contacting police/fire/EMS
- ✓ Duress communication procedures
  - Code words with work or home to communicate an emergency
- ✓ Emergency phone lists (contacts, resources, personnel)
- ✓ Evacuation routes, assembly areas for evacuated personnel and alternates
- ✓ Command post & liaison procedures with police, fire & EMS

For the Office . . .

- ☞ Prepare contingency plans in the event of an emergency - coordinate these plans with the local emergency services.
  - ☞ Ensure that all personnel are familiar with the appropriate section of these emergency plans and their role.
- ☞ Security is everyone's concern. All staff should be aware and abide by security procedures.
- ☞ Report suspicious persons to the appropriate agency.
- ☞ Do not give information on personnel or operations over the telephone to strangers.
- ☞ Place a barrier between staff and the reception area. Visitors/ maintenance personnel should always be escorted.
- ☞ Lock private toilets, unused closets and offices, etc. . .
- ☞ Institute visitor control procedures.
- ☞ Dangerous devices can come in by mail. Ensure that mail receiving personnel are aware what to look for.
- ☞ Be alert for suspicious persons, packages, mail and cars within and near the building.
- ☞ Do not mark parking spaces; vary parking places.

Bergen County Office of Emergency Management
201-634-3100 or www.bcoem.org