

Kansas COOP Exercise – CYBER Attack

Scenario Summary

Background: It is February in **(your city)** it has been a cold winter with a cold spring coming on. Gas prices are rising; food prices are reflecting the current rise in gas prices. Because of the cold winter residents are feeling the pinch in utility and food prices. The National Threat Advisory Level is yellow, where it has remained for almost a full year.

The Event: Over the past several weeks hackers have conducted cyber attacks that affect several parts of the nation's financial infrastructure. Specifically, credit-card processing facilities are hacked and numbers are released to the Internet, causing 20 million cards to be cancelled; automated teller machines (ATMs) fail nearly simultaneously across the nation. Cyber attacks are directed towards Commodity Markets, Law Enforcement Dispatch Centers and Major Power and Light Companies across the region; causing intermittent power disruptions that are affecting **(your facility or building)**.

Segment 1.

It's Monday approximately 09:00 am, most of your employees have arrived to work and are busy with the day's routines. Your department is preparing for an upcoming disaster exercise and you have an Exercise Planning Meeting at 1200. Suddenly there is a blip in the power and your facility goes dark. Past experience shows that battery backup and uninterruptable power supplies (UPS) last for two to three hours before failing.

Questions:

- What are your concerns at this time?
- What contingency plans do you have to in place for this type of event?
- What if power cannot be restored?
- What are your procedures in the event that power cannot be restored?

COOP Capability: Situation assessment procedures--agency administration only, agency wide and outside agency.
COOP Capability: Communications between critical personnel.

Segment 2.

Its 12:00 pm, commercial power has not been restored. It appears that a large portion of your city is without power. Weather is cold and many of your employees have children in the schools in your **(town/city)**. Your facility manager didn't do his routine generator checks and services preparing for cold weather and your backup generator has failed to start up. As the maintenance team struggles to ascertain the problem the school has announced that they were cancelling school due to the power outage.

Questions:

- What are your concerns at this time?
- What contingency planning are you doing?
- What are your Essential Functions or Services that must be continued during this outage?

Kansas COOP Exercise – CYBER Attack

- Are there any considerations for utilizing your COOP?
- How will you implement the plan?
- What are your employee working policies as they pertain to your Essential Functions and Services?

COOP Capability: Situation assessment procedures--agency administration only, agency wide and outside agency.

COOP Capability: Notification Procedures, both internal and external.

COOP Capability: Communications between critical personnel.

COOP Capability: Employee personal and family preparedness.

Segment 3.

Approximately 1:30 pm the maintenance team determines that the backup generator needs repair parts before it can be started and tries to order the parts; but phones and the internet are down. He can run across town and try to order the parts at a local parts house but no one knows if this will be successful. The maintenance supervisor cannot determine when the generator will be repaired at this time. Employees are beginning to complain and many are leaving to pick up their children from school.

Questions:

- What are your concerns at this time?
- What policies are in place to address this situation?
- What if power cannot be restored to your facility?
- Are there any considerations for utilizing your COOP or activating COOP Teams?

Inject#1: Commercial power remains out due to damaged cooling pumps and no indication power will be restored today or tomorrow.

- What are your planning priorities at this time?
- What other considerations would you have if you implement COOP?
- Have you conducted any COOP Relocation Team training recently?
- What preparations have been done relating to your Alternate Facility?

COOP Capability: Notification Procedures, both internal and external.

COOP Capability: Activation and deactivation procedures for COOP teams.

COOP Capability: Alternate facility activation.

Segment 4.

Its 6:30 pm, commercial power is still out and your backup generator is still down and repairs cannot be made tonight. Your building is now cold all employees are at home dealing with their own power problems. Your Crisis Acting Team has to consider options for the next day, week or longer.

Kansas COOP Exercise – CYBER Attack

Inject #2: The FBI has confirmed that this was a Cyber Attack. Locally not only is the power plant down but the water plant has been affected too and the Bank ATM's are also down.

Questions:

- What planning is your CAT Team doing?
- What plans and policies are in place concerning the current situation?
- Are there any considerations for utilizing your COOP or activating COOP Teams?
- How will you communicate your intent to your employee's?
- What is your Alternate Facility Activation Plan?
- What are your Essential Functions and how will you ensure that they are continued to be provided during this event?

COOP Capability: Notification Procedures, both internal and external.

COOP Capability: Activation and deactivation procedures for COOP teams.

COOP Capability: Alternate facility activation.

Decision Point 1: Implement your COOP plan or Not.

Inject #3: It's 1030 pm, your CAT has decided to activate the Alternate Facility plan.

Questions:

- What are your priorities and how do you implement the plan?
- How do you notify your employee's and inform them of your decision?
- Who are your essential employee's? Who are your Relocation Team members and how are they informed about your decision?
- How accurate are your contact rosters and have you conducted any COOP Relocation Team training recently?
- What are your Alternate Facility activation procedures?
- What are your procedures for reduced staffing as your employees deal with their own problems.
-

COOP Capability: Notification Procedures, both internal and external.

COOP Capability: Activation and deactivation procedures for COOP teams.

COOP Capability: Alternate facility activation.

COOP Capability: Employee personal and family preparedness.