Simple Tabletop Exercise, Security Breach – Notification by Witness Account Scenario Scenario #2 Facilitator's Guide

Scenario Summary

Background: It is August in Zenith City, and the hazy heat has left many residents feeling lethargic. However, the city is hosting its 20th annual fair and many residents are taking advantage of the rides, exhibits, contests, games, food, and entertainment that the fair provides. The National Threat Advisory Level is yellow, where it has remained for almost a full year. The city has recently increased its visual inspections of the water distribution system's key components based on both the threat level and the presence of the city's fair, which draws many non-residents to the city.

The Event: On July 27th, painting contractors hired by the Zenith City Water Treatment Plant finish painting the Strawberry Hill Standpipe. One of the painters takes off his latex gloves and throws them down on the platform at the top. He changes out of his painter's suit, packs up his gear, and descends from the top of the tank to catch a ride home with his workmates. The latex gloves are left behind, wedged into the catwalk platform grate.

Early in the morning on August 2nd, a couple of acrobats performing at the fair decide to scale the fence at the water supply tank located near the city fairgrounds. One of the acrobats, dressed in white, throws a grappling hook attached to a climber's rope up to the top of the water tank. He successfully climbs up to the catwalk platform at the top of the tank. He then proceeds to pick the tank hatch's locking mechanism. After successfully breaking into and opening the hatch, he repels down the side of the tank and flees the site. The perpetrator's partner videotapes the entire stunt.

Later that morning, a water utility inspector making her rounds notices that a hatch is open on the top of the Strawberry Hill tank. There are no other indications of a break-in at the tank. Thinking a fellow employee must have accidentally left the hatch open, she unlocks both the perimeter fence and the ladder guard to gain access to the tank. After climbing the ladder to the top of the tank, she notices that a pair of latex gloves is lying to one side of the open hatch, wedged into the platform grate. Not expecting this, she decides to descend from the tank to call her utility manager to report what she has found.

The Results: The emergency rooms around the city note a rise in visits from people from all parts of Zenith City who are complaining of gastrointestinal illness. It is speculated by the media that the illnesses might be related to the security breach at the water tank.

To the Facilitator: The goal of this exercise is to evaluate the ability of the participants to react to a potential threat to a water system in the absence of critical information.

Participants will be required to consider the Threat Evaluation Process (from the Response Protocol Tool Box [RPTB]) to determine how best to handle the "security breach" threat presented in this exercise. The participants will also be required to discuss critical notifications and collaborations required to address the threat scenario in an organized and effective manner.

Intended Participants: This exercise may be run for water supply, public health, state drinking water primacy agencies, federal agencies such as EPA and the Federal Bureau of Investigation (FBI), local law enforcement, and fire/emergency medical services (EMS) personnel. You may wish to consider inviting:

Public Utilities:	Water/Wastewater Utility Managers, Emergency Response Team Members, Utility Operators, IT/SCADA Operators, Engineers, Sampling Staff, Administrative Staff
Hospital:	Emergency Room staff, Physicians, Nurses and Nurse Practitioners, Hospital Administrators, Medical Laboratory staff, Public Information Officer
Public Health:	Health Officers, Epidemiologists, Technical Specialists, Public Information Officer
Fire Dept., HazMat and EMS:	Fire Fighters, HazMat Team members, EMS workers, 911 Call Center workers
Police:	Police Officers, Counter-Terrorism Specialists
Laboratory:	Analysts / Technicians, Laboratory Administrators
Local Officials:	Mayor and Elected Officials, City Council Members, Local Emergency Planning Committee (LEPC) Members, Local Emergency Management Agency staff
State Officials:	State Environmental Agency Staff, State Health Department Staff, State Drinking Water Primacy Agency, State Emergency Management Agency, Governer's Office Representatives
Federal Officials:	EPA staff, FBI staff, FEMA staff, CDC staff, DHS staff

Specifically, water and wastewater utility personnel, local, county and state health officials, and members of the law enforcement community should be involved in the exercise. It would also be beneficial to involve laboratory representatives in the discussions, as they would play a prominent role in a contamination threat scenario of this type.

Running the Exercise

Step 1: Decide on a facility, training date, training duration, and who to invite. Invite participants well in advance of your training date to ensure that you can achieve your attendance goal. Allow adequate time for planning and be sure to prepare all materials (digital and hard copy) ahead of time.

Step 2: Depending on who is participating in this exercise, it may be a good idea to have the participants go around the table and introduce themselves (name, utility, and job title) so that everyone will understand where any particular individual is "coming from" during the ensuing discussions.

Step 3: Explain to the participants that they are participating in a simple tabletop exercise, there is no time pressure, and that they are there as a group to discuss their roles and responses to an emergency incident. There are no right or wrong answers, but the group should be able to discuss problem or "gray" areas that may arise during the exercise. Let them know this is good, as the exercise should stimulate discussion that may lead to changes in the way the participants conduct their daily and emergency operations. Also inform the participants that, although the incident is set in fictional Zenith City, it is okay to talk about the incident from their own experiences or in the context of their own protocols and procedures. It will make the exercise more beneficial for the participants if they exchange emergency response practices, protocols, and procedures that they may currently use.

Step 4: Be sure to give the background PowerPoint® presentation to introduce the participants to Zenith City and to set the stage for the incident. The exercise goals will also be presented as a part of this presentation.

Step 5: Begin the exercise by delivering the first inject. Then, let the discussion evolve naturally on its own after giving the participants the first inject. If necessary, to get the discussion started, simply "nudge" the participants with a non-leading question such as: What would you do in this situation? You could direct this question to the group at large, or, in a group where no one is willing to break the ice, to a particular individual, preferably one that you know serves in a leadership role during the course of their daily activities. You can also refer to the discussion points in the Facilitator's Guide to help jump-start discussion.

Step 6: Be sure to take notes during the discussions. These notes will form the basis of your after-action review. Note problem or gray areas that need more research prior to resolution and who will perform this research or any action items decided upon by the participants. The notes you take will ensure that a summary of the take-home points, action items or messages will not be forgotten or overlooked. You may wish to write these points, action items and messages on a flip chart at the end of the exercise.

Step 7: Perform an after-action review. You may wish to give the participants a 10 to 15 minute break at the end of the exercise to give yourself time to compose your notes prior to conducting the review. Be sure to review the exercise objectives again to determine if the objectives were met by the exercise. Allow the participants to give their feedback on the exercise and the conclusions or decisions that they arrived at during the exercise. The entire tabletop exercise, including the after-action review, can typically be conducted in a two to four hour session. This time range is flexible and is dependant on the amount of discussion generated during the exercise. The pace of the exercise is controlled entirely by the facilitator, who manages the discussions and presents the injects.

Discussion Points

Remember, this scenario begins in the month of August. Many residents of Zenith City are enjoying the summertime activities that the city has to offer, including the city fair, AAA baseball games, and swimming, fishing, and boating on Lake Wobegun. The National Threat Advisory Level is yellow, signifying an elevated threat of terrorist attack. In response to this threat level, the water utility is performing daily security inspections of all facilities, storage tanks and pumphouses as specified by their Emergency Response Plan protocols. Exercise participants are provided a map of Zenith City, a water supply distribution map, a wastewater distribution map, a facilities inspection log, and other pertinent materials. If this exercise is to be customized, all these materials may be substituted with a utility's own maps and other materials.

Inject #1 (11:05 hrs., August 2, Material Code(s) *SSc2-1a* and *SSc2-1b*): *Radio call from a water treatment plant operator performing scheduled daily facilities inspection. The operator reports a tank breach. A tank hatch is found wide open and a pair of used latex gloves are found on the platform beside the hatch.*

Points that could be covered in the discussion of Inject #1 include:

- Was the facilities inspection log used to narrow down when this incident might have occurred? Discuss the importance of conscientiously updating and maintaining security inspection logs, as they are critical in the event of a security breach.
- Discuss if the incident warrants activation of the Emergency Response Plan (ERP) and the utility's internal Chain of Command. Would the current information lead the utility to classify the threat as "Possible" or "Credible" (according to the RPTB Threat Evaluation Process)?
- Discuss appropriate notifications. (e.g. police, health department, hospitals, and possibly FBI)
- Discuss what type of sampling should be performed, who should perform the sampling, and how to select appropriate sampling locations. Would it be wise to call in a qualified HazMat team with appropriate personal protective equipment (PPE) to perform the sampling, as the nature of the potential contamination threat is unknown?

Inject #2 (14:15 hrs., August 2, Material Code(s) *SSc2-2*): *A phone call from the health department to the water utility informs them that the local hospitals are reporting multiple similar gastrointestinal illness cases in the past 24 hours. The health department is assuming that illnesses are either food- or water-related and they are requesting follow-up.*

Points that could be covered in the discussion of Inject #2 include:

- Would the health department normally notify the water department of an illness outbreak?
- Discuss whether this new information is enough to promote the threat evaluation to a "Credible" stage (according to the RPTB Threat Evaluation Process)
- Discuss if analytical tests on the water should be more focused on biological contaminants, based on the new information provided by the health department. Is it wise to narrow the focus of the sampling and testing without confirmation that the apparent "cause" (the tank breach) and "effect" (multiple gastrointestinal [GI] illness cases) are related?
- Should the tank be isolated at this point?
- Should the FBI be informed of this incident? How do the new National Response Plan (NRP) and National Incident Management System (NIMS) affect your decisions?
- What is the proper time to inform the public, and what is the best way to disseminate information? The water utility should have assigned a public information officer (PIO) as part of the development of the command group in their ERP. This is the person tasked with disseminating controlled and accurate information to the media and the public.
- When would the wastewater plant be notified?

Inject #3 (14:35 hrs., August 2, Material Code(s) *SSc2-3*): *A news station reports that a source from the water utility has leaked to them the details of the tank break-in. The media speculates that the water supply may be contaminated.*

Points that could be covered in the discussion of Inject #3 include:

- Discuss how to handle public perception in the aftermath of this alarmist news report. Consumer confidence will be severely reduced. What steps should be taken to restore consumer confidence?
- Discuss how to handle minimizing information leaks from the utility or other agency staff members.

Inject #4 (9:30 hrs., August 3, Material Code(s) *SSc2-4*): *Phone call from the health department to the water utility informing them that several more GI illness cases have been reported in emergency rooms across the city.*

Points that could be covered in the discussion of Inject #4 include:

- In light of this new information, and in the absence of laboratory results (as confirmation from most biological tests take 24-48 hours), should a "boil", "do not drink", or "do not use" order be issued?
- Discuss preventative measures such as hyper-chlorination and system flushing as viable options for dealing with the potentially contaminated supply.
- At this point in the scenario, how is incident command structured? Is the incident commander a member of the police or public health? Are two simultaneous command structures required to deal with the two separate incidents, since they are not necessarily related (i.e. the security breach/potential contamination threat and the GI illness outbreak)? Is a Unified Command appropriate?

Inject #5 (10:30 hrs., August 3, Material Code(s) *SSc2-5*): *A news station reports that a source at the hospital has informed them that GI illness cases are flooding the ER, and that the cause of the illnesses is likely food-borne or water-borne (based on the symptoms). The news reporter goes on to speculate that the tank security breach on August 2 could be a deliberate attempt to contaminate Zenith City's water.*

Points that could be covered in the discussion of Inject #5 include:

- How should the media be handled in a crisis situation? Often, the media will speculate or deliver inaccurate information to the public. Discuss how best to handle this type of situation.
- Should gag orders be implemented at the utility, the hospitals, etc. to minimize misinformation leaks to the media and the public?
- Reinforce the importance of accurate and controlled information dissemination to the public.
- What "media plans" do the participants have in place in their own utilities?

Inject #6 (13:50 hrs., August 3, Material Code(s) *SSc2-6*): *Phone call to police from eyewitness. A teenager on his way to work at the fair witnessed suspicious activity at the Strawberry Hill water tank yesterday morning. He reports what he observed.*

Points that could be covered in the discussion of Inject #6 include:

- In light of this new information, what response actions may need to be taken?
- Who should be notified of this information? Discuss the need to notify Incident Command, which should result in notification of all the parties involved (the FBI, the utility, the health department, etc.)
- If the threat stage is still considered to be "Possible," does this eyewitness testimony advance the threat to the "Credible" stage? The "Confirmed" stage?

Inject #7 (16:30 hrs., August 3, Material Code(s) *SSc2-7a* and *SSc2-7b*): *Lab results confirm that water samples collected by the utility and/or HazMat are clean.*

Points that could be covered in the discussion of Inject #7 include:

- Discuss the possibility that the appropriate analytical tests may not have been performed. Reinforce that negative results do not necessarily confirm that the water supply is "clean".
- Should a second sampling round be performed to reinforce the first round of analytical results?
- Does this information indicate that the illnesses may most likely be food-related?
- Should health officials be notified of these results?
- Should the media be notified of these results?
- If representatives are present from lab facilities, ask them how they approach sampling for the "unknown" and what the utility can do to make things easier for the lab.

Inject #8 (17:40 hrs., August 3, Material Code(s) *SSc2-8*): *Email from a health department official to the utility confirming that illnesses were caused by a group of food vendors at the fair. Many residents of Zenith City consumed improperly prepared food from this vendor and were exposed to Salmonella bacteria.*

Points that could be covered in the discussion of Inject #8 include:

- Discuss whether this information is enough to dismiss the threat of contamination to the water supply.
- Should the supply tank be returned to service (if it was isolated during the incident)?
- Reinforce that consumer confidence will need to be restored. The role of the utility's PIO is critical during this recovery step.

Inject #9 (18:00 hrs., August 3, Material Code(s) *SSc2-9*): *Telephoned confession to police from the perpetrator. A carnival performer working at the city fair confesses to climbing the water tower and breaking into the tank as a stunt. He provides video footage to prove to authorities that he did not contaminate the supply.*

Points that could be covered in the discussion of Inject #9 include:

- What types of security measures could be implemented to avoid this type of breach? Are these measures feasible from the standpoint of financial and resource constraints?
- How does a utility recover from an intentional incident such as this one? The response procedures and efforts can be costly to a utility's funds and resources.
- How does a healthy relationship with the media benefit the utility and first responders in an event such as this one?
- What steps have the participants taken to create a relationship with the media in their local community?