

**Simple Tabletop Exercise, Cyber Security Breach –
Unusual Water Quality Scenario
Scenario #3
Facilitator’s Guide**

Scenario Summary

Background: It is summer in Zenith City. The end of the city’s fiscal year is approaching, and budgetary cutbacks within the city and the water department have resulted in several city employees being laid off.

The Event: A water (or wastewater) utility worker, angry that he has lost his job, realizes that he is still able to dial-in to the Zenith City Water (or Wastewater) Treatment Plant’s SCADA system. He decides to infect the SCADA system with a computer virus to cause system malfunctions.

The Results: The SCADA system begins to issue alarms that inform operators that various systems in the treatment process are malfunctioning, and that water (or wastewater) leaving the treatment plant is not meeting water quality standards for drinking (or discharge). The SCADA system also reports malfunctions with the process flow routing and chemical feed rates.

To the Facilitator: Because these alarms are computer virus-induced, they do not reflect the actual operation of the system. However, the exercise participants will not be aware of this fact until later in the exercise. This exercise is intended to generate discussion among the utilities represented regarding security procedures and protocols for SCADA systems and to gauge how confident personnel feel in operating their utilities without the aid of SCADA systems.

This exercise may be run for either water or wastewater utility personnel, and appropriate suggestions for injects based on the exercise participants are included throughout this guide. In general, the terminology to be used for a wastewater audience can be found in parentheses immediately following the drinking water terminology. See the description for Inject #1 below for an example.

Intended Participants: This exercise may be run for water supply, wastewater operators, public health, state drinking water primacy agencies, federal agencies such as EPA and 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, Governor's Office Representatives |
| Federal Officials: | EPA staff, FBI staff, FEMA staff, CDC staff, DHS staff |

Specifically, water and/or wastewater utility personnel, water and wastewater utility Information Technology (IT) personnel (if applicable), representative(s) from the utility's contracted IT firm or service (if applicable) should be included in this exercise.

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 after the end of the city's fiscal year, and budgetary cutbacks within the city and the water department have resulted in several city employees not being able to return to work. A water (or wastewater) utility worker, angry that he has lost his job, realizes that he is still able to dial-in to the Zenith City Water (or Wastewater) Treatment Plant's SCADA system. He decides to infect the SCADA system with a virus that will make it malfunction. Exercise participants are provided a map of Zenith City, a water supply distribution map, a wastewater distribution map, 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.

Use injects labeled with an "a" for a water utility audience and injects labeled with a "b" for a wastewater utility audience.

Inject #1 (10:00 hrs., July 10, Material Code(s) SSc3-1a or SSc3-1b): *The SCADA system alerts the operator that two high-lift pumps (or blowers if the exercise involves wastewater personnel) are not operational. The flow meter (or oxygen monitor) indicates that all is normal.*

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

- What is the procedure used to manually/visually inspect the pumps (or blower)?
- Where is this procedure or policy written and kept?
- Does anyone need to be notified?
- What do you do if the person you need to notify is out on vacation?
- Does it matter if this alarm occurs after business hours?

Inject #2 (10:10 hrs., July 10, Material Code(s) SSc3-2a or SSc3-2b): *A physical check of the high lift pumps (or blowers) shows that they are operational.*

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

- How do you know if the pumps (or blower) are operating at the correct rates? Do you assume that the flow meter (or oxygen monitor) is operating correctly?
- What is the appropriate evaluation and repair procedure for high-lift pump monitors within the SCADA system?
- Who is in charge of ensuring that the repair is made?

Inject #3 (10:23 hrs., July 10, Material Code(s) SSc3-3a or SSc3-3b): *The SCADA system alerts the operator that the chlorinator is not working properly, which may lead to out-of-compliance water quality standards. The residual analyzer indicates that nothing is wrong.*

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

- What is the procedure used to inspect the chlorinator?
- How often are personnel trained in this procedure?
- Is there a checklist to take personnel through this procedure?
- How often are personnel trained in any procedure involving troubleshooting the SCADA system?
- What is the back-up plan if the person who knows the SCADA system best is out of town or otherwise not available?

Inject #4 (10:30 hrs., July 10, Material Code(s) SSc3-4a or SSc3-4b): *A physical check of the chlorinator shows that it is operational.*

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

- How do you know that the chlorinator is feeding the right amount of chlorine?
- How much do you trust the residual monitor and the entire SCADA system after the occurrence of what appear to be two false alarms?
- When would sampling be performed to independently verify what the SCADA system is telling you?

Inject # 5 (10:37 hrs., July 10, Material Code(s) SSc3-5a or SSc3-5b): *Results of “grab” water sample (indicating that chlorine residual level is within normal range).*

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

- Is this enough information to assume that the SCADA system is giving false alarms?
- Who would be notified at this point?
- If there is not a full-time Information Technology (IT) staff member, how quickly could the contractor respond to examine the SCADA system?
- What exactly would be done at this point?

Inject #6 (10:47 hrs., July 10, Material Code(s) SSc3-6a or SSc3-6b): *The SCADA system alerts the operator again that the chlorinator is not feeding properly, raising the risk for a second time (within a matter of minutes) that water may be exiting the plant that does not meet water quality standards.*

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

- Why might the SCADA system be alerting the operator yet again that the chlorine feed is not operating properly?
- What do the plant's policies or guidelines say to do in this situation?
- Is water quality sampling being performed to ensure that water leaving the plant meets water quality and/or permit guidelines?
- Are sampling points pre-determined? If not, how do you decide where to sample?

Inject #7 (11:00 hrs., July 10, Material Code(s) SSc3-7a or SSc3-7b): *A physical check of the chlorinator shows that it appears to be operational.*

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

- Would you sample again for chlorine residual (this was just done 20 minutes ago)?
- When is the call made to not use the SCADA system and to go to manual control?
- How often does the utility train to operate the system manually?
- What is the procedure to shift to manual control? Unplug the SCADA?
- Are there any back-up systems that may be employed independent of the SCADA system?
- When do you ask for help from Information Technology (IT)?
- Do you begin to consider that an intentional disruption of the SCADA system is possible? What types of information would you need to gather to make that determination?

Inject #8 (11:15 hrs., July 10, Material Code(s) SSc3-8a or SSc3-8b): *The utility's IT person or IT contractor has discovered that Eric Harwood, a young utility employee recently laid off due to budget cutbacks, accessed the SCADA system remotely after his layoff.*

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

- Who has access to the SCADA system and at what security levels may they access the system?
- Is there a written policy governing SCADA access?
- What are the utility's security procedures and protocols governing SCADA systems?
- Have they been updated since 9/11? Have they been updated within the context of the new National Response Plan (NRP) and National Incident Management System (NIMS)? Why or why not?
- What are the in and out-processing requirements when a new employee is hired or leaves, whether it is a voluntary or non-voluntary separation?
- Are passwords, log-ins, and email accounts cancelled and reassigned?
- Does the fact that the SCADA system was accessed remotely by a former employee lead you to deem this threat "credible"?
- What types of information would you need to confirm this threat?

Inject #9 (11:48 hrs., July 10, Material Code(s) SSc3-9a or SSc3-9b): *The utility's IT person or contractor cannot pinpoint any definitive problem with the SCADA's systems software. In the meantime, the SCADA system has warned of another high-lift pump (or blower) failure. A virus is suspected.*

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

- Based on the knowledge that Eric Harwood was laid off, that he accessed the SCADA system after being laid off, he was upset about his layoff, and the bizarre behavior of the SCADA system which the IT professional says could be a virus, is it time to notify law enforcement? (*Note: As a facilitator, you may wish to re-emphasize with the participants that it is now a federal crime to threaten or tamper with a public drinking water system.*)
- In light of this new information, what would your immediate response actions be?
- With a suspected virus, is it just better and safer to run the entire operation manually? Is this possible?
- What pros and cons need to be balanced in terms of making a decision to operate completely manually versus continuing to use the SCADA and risking the virus affecting some previously unaffected utility component, some other interconnected system or water or effluent quality?
- Can the participating utilities run their system manually?
- How many times has this been trained?
- Is a written procedure or checklist in place to do this?

Inject #10 (13:00 hrs., July 10, Material Code(s) SSc3-10a or SSc3-10b): *Eric Harwood's former supervisor, upon hearing that the problems with the SCADA system may be virus-related and connected to Eric, steps forward to let the water or wastewater superintendent know that he isn't sure if Eric returned his keys to anyone when he left.*

Points that could be covered in the discussion of Inject #10 include:

- What is the utility's key control policy?
- Can keys be easily copied?
- How often are locks changed?
- Is it possible that Eric did more than just plant a virus within the SCADA system?
- Should a physical check of all major plant processes and chemicals be undertaken?
- Who's in charge of inactivating user names and passwords as personnel changes occur?

Inject # 11 (15:27 hrs., July 10, Material Code(s) SSc3-11a or SSc3-11b): *The police, who are looking for Eric for questioning, notify the water or wastewater superintendent that Eric has a criminal record.*

Points that could be covered in the discussion of Inject #11 include:

- How does this change the utility's view of the situation in terms of urgency and seriousness?
- Do the participating utilities have a requirement for a criminal background check of their employees or are they considering instituting such a requirement?