2024

THREATGEN®
AUTOTABLETOP

MWAA – OT Water Utility Scenario

FOR USAGE WITH THREATGEN'S AUTOTABLETOP™

ROBERT C. RHODES

DEREZZED INC. D/B/A THREATGEAN | 118 Vintage Park Blvd., Suite 700 W, Houston, Texas 77070

MWAA - OT Water Utility Scenario

For ThreatGEN AutoTableTop™

Contents

Summary 2

Cybersecurity in the Water Utility Industry 2

The Attack 3

Impact & Response 4

Aftermath and Lessons Learned 4

AutoTableTop Settings 6

Threat Scenario 6

Company Information 6

Department 6

Exercise Objectives 7

General Objectives 7

Participants 8

General Roles for Participants 8

IT Staff 9

General IT Staff Roles 9

OT Staff (If Applicable) 10

General OT Roles 10

Cybersecurity Staff 10

General cybersecurity roles 11

Leadership Staff 11

Network Environment 11

Injects 12

General injects in cybersecurity tabletop exercises 12

Conclusion Settings 12

Summary

Cybersecurity in the Water Utility Industry

The water utility industry has experienced several significant operational technology (OT) cybersecurity breaches in recent years, highlighting the vulnerabilities in critical infrastructure. Here are some of the most important incidents:

Company & Date	Description
American Water Breach **October 2024**	American Water, the largest water utility in the United States, fell victim to a cyberattack that forced the company to shut down its customer portal and pause billing operations [1] [5]. While water and wastewater facilities were reportedly not impacted, this incident underscores the potential risks to OT systems in large-scale utilities. The attack affected services for over 14 million people across 14 states and 18 military installations [3].
Veolia North America Incident **January 2024**	Veolia North America, an international company specializing in water, waste, and energy management, experienced a cyberattack that led to the shutdown of targeted back-end systems and servers [2]. While water treatment operations were not directly impacted, the incident caused service degradation in online bill payment systems and resulted in the theft of personally identifiable information.
Municipal Water Authority of Aliquippa Attack **November 2023**	In this incident, attackers compromised an internet-connected controller used to maintain water pressure within the system [2]. The breach exploited default settings and a simple, publicly known password. Although the authority had access to a manual backup system, this **attack demonstrates the vulnerabilities in operational technology within smaller water utilities.**
Águas e Energia do Porto Breach **January 2023**	This Portuguese water utility suffered a cyberattack resulting in data exfiltration and customer service disruptions [2]. The incident highlighted the potential for hackers to exploit third-party IT service providers to gain access to water utility systems.
South Staffordshire PLC Attack **July 2022**	The UK-based water company experienced a cyberattack that led to the theft of personally identifiable information and disruption to its corporate network [2]. While the safe supply of water to 1.6 million customers was not affected, the incident raised concerns about the potential access to SCADA systems by malicious actors.
Oldsmar Water Treatment Facility Incident **February 2021**	This attack is **significant due to its potential impact**. An attacker gained unauthorized access to the water treatment system in Oldsmar, Florida, and attempted to increase the sodium hydroxide levels to dangerous amounts. Fortunately, an operator noticed the change and prevented any harm [8]. *Subsequently, the incident was reclassified by the FBI and former Oldsmar City Manager Al Braithwaite later stated that the incident was likely not a cyberattack but rather an employee error.*

Table 1 - Water Utility incidents and breaches in the last 6 years

These incidents highlight the increasing frequency and severity of cyberattacks targeting water utilities [9]. The EPA has warned that approximately 70% of inspected water systems failed to meet cybersecurity standards, emphasizing the urgent need for improved defenses in this critical sector [7] [8].

Due to the significance of the Municipal Water Authority of Aliquippa Attack, we have chosen this as the scenario for the water utility industry.

Citations:

1) https://securityintelligence.com/news/cyberattack-on-american-water-warning-critical-infrastructure/
2) https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/
3) https://www.bankinfosecurity.com/largest-us-water-utility-hit-by-cybersecurity-incident-a-26478
4) https://www.insurancebusinessmag.com/us/news/cyber/small-texas-towns-targeted-in-series-of-international-cyberattacks-on-water-systems-486072.aspx
5) https://www.cnbc.com/2024/10/08/american-water-largest-us-water-utility-cyberattack.html
6) https://www.esecurityplanet.com/trends/american-water-cybersecurity-breach/
7) https://www.newsweek.com/drinking-water-warning-issued-epa-millions-customers-1989511
8) https://www.mcglinchey.com/insights/cyberattacks-against-u-s-water-supplies-on-the-rise-epa-urges-utilities-to-fortify-defenses/
9) https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/

The Attack

The Company: The Municipal Water Authority of Aliquippa (MWAA) is a public utility that provides water service to residents and businesses in Aliquippa, Pennsylvania, and surrounding areas. The MWAA water system serves approximately 6,615 customers within the City of Aliquippa and portions of Hopewell Township, Potter Township, and Raccoon Township.

The Attack: On November 25, 2023, the MWAA experienced a cyberattack targeting one of their booster stations. The attack was attributed to an Iranian-backed hacker group known as Cyber Av3ngers. The hackers gained control of a Unitronics Vision Series programmable logic controller (PLC) at the booster station, which monitors and regulates water pressure for Raccoon and Potter Townships.

Impact & Response

The impact of the attack was relatively limited:

- ✓ No customers lost access to water [3].
- ✓ There was no known risk to the drinking water or water supply [2].
- ✓ The affected station was located on the outskirts of town and only regulated pressure for specific areas [2].

The MWAA's response to the attack was swift:

- An alarm was triggered immediately when the hack occurred [2].
- The authority quickly disabled the affected system and switched to manual operations [6].
- Pennsylvania State Police were called to begin a criminal investigation [2].
- Federal authorities, including the Cybersecurity and Infrastructure Security Agency (CISA), became involved in the investigation [6].

Aftermath and Lessons Learned

The Aliquippa cyberattack highlighted several critical issues in cybersecurity management for water utilities and other critical infrastructure:

1) **Vulnerable Control Systems**: The attack exposed weaknesses in PLC security, particularly those manufactured by Israeli companies, which were specifically targeted by the hackers [2] [6].
2) **Poor Password Security**: CISA reported that the hackers likely exploited weak password security, possibly even using a default password [3] [6].
3) **Internet Exposure**: The compromised PLC was directly exposed to the internet, making it an easy target for cyberattacks [6].
4) **Need for Multi-Factor Authentication**: The incident underscored the importance of implementing multi-factor authentication for remote access to operational technology networks [6].
5) **Importance of System Updates**: Keeping PLC firmware and software up-to-date was identified as a crucial step in preventing similar attacks [6].
6) **Backup and Recovery**: The need for backing up PLC logic and configurations to enable fast recovery was emphasized [6].
7) **Cybersecurity Awareness**: The attack raised awareness about the potential risks to critical infrastructure and the need for improved cybersecurity measures in water treatment facilities [7].

In response to this incident, CISA issued recommendations for securing water and wastewater facilities against similar vulnerabilities, including changing default passwords, implementing firewalls, and updating firmware [6]. The attack serves as a wake-up call for water utilities and other critical infrastructure operators to reassess and strengthen their cybersecurity practices.

Citations:

1) https://hopewelltwp.com/directory/municipal-water-authority-of-aliquippa/
2) https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/
3) https://triblive.com/local/regional/municipal-water-authority-of-aliquippa-falls-victim-to-cyberattack-feds-say/
4) https://securityaffairs.com/154818/hacktivism/cyber-av3ngers-hacked-municipal-water-authority-of-aliquippa.html
5) https://aliquippawater.com
6) https://www.waterworld.com/water-utility-management/article/14302077/aliquippa-pennsylvania-suffers-cyberattack-on-booster-station-plc
7) https://blueridgenetworks.com/aliquippa-water-authority-attack-analysis

AutoTableTop Settings

Threat Scenario

Company Information

Company Name:	**Municipal Water Authority of Aliquippa**
Company Description:	**Public water utility serving approximately 6,615 customers in Aliquippa, PA and surrounding areas**

Department

Based on best practices for tabletop exercises, we recommend including 2-3 key departments in a live tabletop exercise for the **Municipal Water Authority of Aliquippa – in this case just "Water Operations" and "IT"**. This number allows for comprehensive coverage of critical areas while keeping the exercise manageable and focused. The most appropriate departments to include would be:

1) Information Technology (IT) / Cybersecurity Team
2) Operations Management
3) Executive Leadership
4) Legal Department
5) Public Relations / Communications

If resources allow, you could also consider adding:

6) Human Resources
7) Finance/Accounting

This selection ensures representation from technical, operational, and business aspects of incident response. It allows for a well-rounded approach without overwhelming participants or diluting the exercise's effectiveness [1] [4]. Including these departments enables the exercise to cover key areas such as:

- Technical response and investigation
- Operational impact and mitigation
- High-level decision making
- Legal and regulatory considerations
- Internal and external communications
- Financial implications

Remember, the goal is to create a collaborative environment where participants can discuss their roles and responses effectively [2]. Starting with a core group of 2-4 departments provides a solid foundation for a productive tabletop exercise, allowing for meaningful interaction and decision-making processes to be tested.

Citations:

1) https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf
2) https://www.csoonline.com/article/570871/tabletop-exercises-explained-definition-examples-and-objectives.html
3) https://www.calhospitalprepare.org/post/what-difference-between-tabletop-exercise-drill-functional-exercise-and-full-scale-exercise
4) https://www.police1.com/police-training/articles/virtual-tabletop-exercise-public-safety-leaders-demonstrate-importance-of-interagency-training-mlzzUdW2rX2EMHXW/
5) https://campusguard.com/post/cybersecurity-tabletop-exercises-for-leadership-teams/
6) https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/
7) https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
8) https://www.reddit.com/r/k12sysadmin/comments/1095zud/cybersecurity_tabletop_exercises/

Exercise Objectives

Here are the specific objectives that integrate with the scenario’s real-life aftermath and lessons learned:

1) **Test response to PLC compromise.**
2) **Evaluate manual operation procedures**
3) **Assess cybersecurity measures for OT systems.**

General Objectives

Here are some examples of effective tabletop exercise objectives:

1) Assess the communication plan during a data security breach.
2) Practice resource allocation and decision-making during a natural disaster.
3) Identify gaps in the business continuity plan following a power outage.
4) Evaluate the effectiveness of the evacuation plan in response to a fire alarm.
5) Improve collaboration among departments in a product recall scenario.
6) **Test the incident response plan for the Municipal Water of Aliquippa.**
7) Evaluate the organization's ability to coordinate with external stakeholders during a crisis.
8) Assess the team's readiness and knowledge in responding to a specific emergency scenario.
9) Test new or updated emergency procedures.
10) Improve response time and effectiveness compared to previous tabletop exercise performances.

When crafting objectives for a tabletop exercise, it's important to make them SMART (Specific, Measurable, Achievable, Relevant, and Time-bound). The objectives should be clearly defined and align with the organization's goals for emergency preparedness and response. They should also be tailored to the specific scenario being simulated and focus on key aspects of the response plan that need evaluation or improvement.

List of relevant sources:

1) https://www.alertmedia.com/blog/tabletop-exercises/
2) https://www.ravemobilesafety.com/blog/tips-conducting-effective-tabletop-exercise/
3) https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf
4) https://securityscorecard.com/blog/what-are-tabletop-exercises/
5) https://nexightgroup.com/9-steps-to-design-a-powerful-tabletop-exercise/
6) https://www.csoonline.com/article/570871/tabletop-exercises-explained-definition-examples-and-objectives.html
7) https://www.alertmedia.com/blog/tabletop-exercise-scenarios/
8) https://www.csoonline.com/article/518982/tabletop-exercise-scenarios.html

Participants

For this scenario, these are the valid participants associated with the water utility:

- **Water operations staff,**
- **IT personnel,**
- **cybersecurity team, and**
- **leadership**

ThreatGEN is not aware of the exact company positions within the Municipal Water Authority of Aliquippa that participated in the handling of the incident; however, these are the individuals in the organization at the time of the incident:

Board of Directors

- Matthew Mottes, Chairman
- Jason Stauffer, Vice Chairman
- Wilbur Moreland, Secretary
- Heather Vono, Assistant Secretary / Treasurer

Management

- Robert J. Bible, PE, General Manager

Matthew Mottes, as the Chairman of the Board of Directors, was actively involved in communicating about the incident to the media and working with federal authorities during the investigation. Robert J. Bible, the General Manager, also provided statements about the cyberattack and its impact on the utility's operations.

While specific IT, cybersecurity, and water operations staff were not named in the search results, these leadership figures were key in managing the response to the incident and coordinating with law enforcement and cybersecurity agencies.

General Roles for Participants

Based on the recommended departments for a tabletop exercise in a similar setting, here's a list of possible individual participants' titles:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- IT Security Manager
- Network Administrator
- Chief Operating Officer (COO)
- Pipeline Operations Manager
- Control Room Supervisor
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- General Counsel
- Compliance Officer
- Public Relations Director
- Corporate Communications Manager
- Human Resources Director
- Risk Management Officer
- Emergency Response Coordinator
- Business Continuity Manager
- Incident Response Team Lead
- Cybersecurity Analyst
- Digital Forensics Specialist
- Customer Service Manager
- Supply Chain Manager
- Environmental Health and Safety Manager
- Government Relations Director
- Board Member (if applicable)

This list covers a range of roles across different departments, ensuring a comprehensive representation of key decision-makers and subject matter experts. Depending on the specific goals of your exercise and the size of your organization, you may choose to include all or a subset of these roles.

IT Staff

For this scenario, these are the IT staff positions that we assume were involved in responding to the incident:

- **Network administrators**
- **System engineers**

General IT Staff Roles

Here's a list of high-level roles in the IT department that could be included:

1) Chief Information Officer (CIO)
2) Chief Information Security Officer (CISO)
3) Chief Technology Officer (CTO)

4) IT Director
5) IT Security Manager
6) Network Architecture Manager
7) Infrastructure Manager
8) Applications Manager
9) Database Manager
10) IT Operations Manager
11) IT Project Manager
12) Incident Response Team Lead
13) Cybersecurity Analyst Lead
14) Cloud Services Manager
15) Data Center Manager

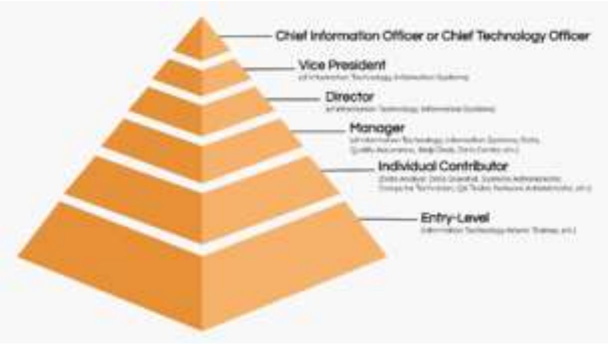

Figure 1 - General IT staff involved

These roles represent key decision-makers and leaders within the IT department who would likely be involved in responding to a major cybersecurity incident. They cover various aspects of IT operations, security, infrastructure, and management that would be crucial in addressing a ransomware attack or similar threat to critical systems.

OT Staff (If Applicable)

These are the specific staff that we know were involved in the response:

- **Water treatment operators**
- **Maintenance technicians**

General OT Roles

Here is a general list of OT (Operational Technology) staff that might be found in many companies, and then suggested specific roles that are relevant:

1) Chief Information Officer (CIO)
2) Chief Technology Officer (CTO)
3) OT Manager
4) OT Security Manager
5) Control Systems Engineer
6) SCADA Engineer
7) Industrial Control Systems (ICS) Specialist
8) Automation Engineer
9) Network Engineer (OT focus)
10) OT Security Analyst
11) OT Systems Administrator
12) OT Project Manager

Cybersecurity Staff

These are the specific staff that we believe would be part of the response team for MWAA:

- **Security Analysts**

- **Incident responders**

General cybersecurity roles

Here is a list of general cybersecurity roles and suggestions of some specific roles that would likely be relevant for any scenario:

1) Chief Information Security Officer (CISO)
2) Information Security Manager
3) Cybersecurity Analyst
4) Incident Response Specialist
5) Penetration Tester/Ethical Hacker
6) Security Operations Center (SOC) Analyst
7) Network Security Engineer
8) Application Security Specialist
9) Cloud Security Architect
10) Compliance Specialist

Specific cybersecurity roles likely relevant for Colonial Pipeline:

1) Pipeline Cybersecurity Manager
2) Industrial Control Systems (ICS) Security Specialist
3) SCADA Security Engineer
4) OT/IT Security Integration Specialist
5) Cybersecurity Incident Response Coordinator
6) Critical Infrastructure Protection Analyst
7) Ransomware Prevention Specialist
8) Supply Chain Security Analyst
9) Cyber Threat Intelligence Analyst (focused on energy sector threats)
10) Security Awareness Training Coordinator

Figure 2 - General roles in cybersecurity

Leadership Staff

The leadership staff known to be involved in the response to this incident were:

- **Robert J. Bible, PE, General Manager**
- **Operations Manager**
- **Public Relations Officer**

Network Environment

This is the general layout for the MWAA network:

- **OT network with internet-connected PLCs,**
- **SCADA systems, and**
- **manual backup controls**

Injects

Here are some specific injects tailored for a cybersecurity tabletop exercise for this water utility (MWAA), followed by some general injects:

- **Alarm triggered for unauthorized PLC access,**
- **Pressure readings show unusual fluctuations,**
- **Cyber Av3ngers claim responsibility on social media**

General injects in cybersecurity tabletop exercises

- An employee reports receiving a suspicious email with an attachment.
- The IT team detects unusual network traffic from a server.
- A critical system suddenly becomes unresponsive.
- An external partner reports a potential data breach involving shared information.
- Social media posts claim to have accessed sensitive company data.
- Ransomware messages appear on multiple workstations.
- A phishing campaign targets executives with fake login pages.
- An insider threat is suspected based on unusual data access patterns.

These injects are designed to test the incident response capabilities of various departments, including IT/cybersecurity, operations, executive leadership, legal, and public relations. They simulate the escalating nature of a cyber incident and require participants to make decisions, communicate effectively, and manage both technical and business aspects of the crisis.

Conclusion Settings

These are the settings that we have suggestions for but your specific goals for your tabletop exercise would dictate changing these to meet your needs. Experiment!

Win Conditions:	**1) PLC compromise detected and contained** **2) Manual operations successfully implemented** **3) Public water supply remains unaffected**
Loss Conditions:	**1) Failure to detect PLC compromise** **2) Disruption in water pressure regulation** 3) **Delayed public communication about the incident**
Additional Instructions:	Emphasize the importance of password security, multi-factor authentication, and air-gapping critical systems.
Industry:	Water Utility