ThreatGEN® AutoTableTop 2.0

2026 WATER UTILITY COMPETITION

Post-Competition Study

Abstract

This case study compares 20 controlled trials by ThreatGEN® technical staff against 16 teams of water/wastewater operators, all running the same AutoTableTop™ 2.0 ransomware scenario. Tool-familiar staff scored more consistently (6.5 vs. 6.1 average), but operators with zero platform experience produced the highest single score of either group (8.0) and surfaced operationally authentic actions no tool expert considered. The findings validate that AutoTableTop™ 2.0 accurately evaluates crisis management competence independent of cybersecurity knowledge, and that domain expertise, when paired with even brief tool orientation, outperforms tool familiarity alone.

Robert C. Rhodes
robert@threatgen.com

Executive Summary

This case study compares the performance of two fundamentally different user populations on the same AutoTableTop™ 2.0 ransomware crisis management exercise for a Texas water treatment facility. The first group, ThreatGEN's technical support team, conducted 20 pre-competition study trials with deep knowledge of the tool but no water/wastewater industry experience. The second group, 16 participating teams at the 2026 water industry operations event, are working water and wastewater operations professionals with no prior exposure to AutoTableTop™ and generally limited cybersecurity knowledge.

Note: Team names and identifying details have been anonymized at the request of the event management. All scores, transcripts, and After-Action Report findings are presented exactly as generated by AutoTableTop™ 2.0.

The central question: Does knowing the tool or knowing the industry produce better crisis management outcomes?

The answer, supported by the data, is that neither advantage alone is sufficient - but the combination of domain expertise with even brief tool orientation produces the highest-quality results. The event's top-performing team (Clearwater All-Stars) achieved a perfect 8.0 average across 4 turns, the highest average score of any trial in either group, demonstrating that operators who grasp the exercise format can leverage their operational instincts to outperform tool-familiar participants.

Study Design

Group A: Technical Support Team (Pre-Competition Study)

- 20 trials conducted prior to the event
- **Participants**: ThreatGEN technical support staff with deep AutoTableTop™ 2.0 platform knowledge
- **Industry knowledge**: None, no water/wastewater operational experience
- **Tool familiarity**: Expert, understood scoring mechanics, phrasing optimization, turn count strategy
- **Scenario parameters**: "*Surprise me*" for most fields; standard verbosity; detailed objectives
- **Approach**: Iterative optimization over 20 runs to identify highest-scoring input phrasings

Group B: Competition Teams (Live Event)

- 16 teams competing at the 2026 water industry operations event
- **Participants**: Water and wastewater plant operators, maintenance technicians, laboratory and collection systems staff

- **Industry knowledge**: Expert, daily operational experience with water treatment, SCADA, HMIs, and plant processes
- **Tool familiarity**: None, first exposure to AutoTableTop™ 2.0 at the event
- **Scenario parameters**: Minimalist configuration (most fields blank); concise verbosity
- **Approach**: Real-time, unscripted responses under event time pressure (approximately 30 min slots)

Competition Results

AutoTableTop™ 2.0 scores each participant turn on a 0 to 10 scale. A score of 10 is rarely awarded and represents an exceptional, textbook-quality crisis management action. The event awarded trophies to the top three teams with the highest cumulative total score (sum of all per-turn scores), rewarding both quality and depth of engagement. The following table presents both total and average metrics:

#	Team Name	Turns	Total	Avg	High	Low
1	Lone Star Operators	5	31	6.2	7	5
2	Basin City Legends	6	38	6.3	7	5
3	Clearwater All-Stars	4	32	8.0	8	8
4	Headworks Heroes	3	19	6.3	7	6
5	Aeration Aces	4	22	5.5	8	3
6	Floc Squad Alpha	6	36	6.0	8	4
7	Turbidity Titans	10	67	6.7	8	5
8	Grit & Grind Crew	4	26	6.5	7	5
9	Chlorine Kings	14	94	6.7	8	5
10	Effluent Eagles	3	19	6.3	8	4
11	Microbe Mavericks	5	33	6.6	8	5
12	Settling Basin Squad	8	33	4.1	7	0
13	Team Weir Gate	3	17	5.7	7	5
14	Pump Station Posse	5	31	6.2	8	5
15	Sludge City Senders	6	38	6.3	8	5
16	Team Backwash	2	10	5.0	5	5

** Remember that all team names have been anonymized per event management requests.

Comparative Analysis

Scoring Performance

Metric	Group A (Tech Support)	Group B (Operators)
Number of trials/teams	20	16
Average score (mean of averages)	6.5	6.1
Highest individual avg score	7.5 (Trial A19)	8.0 (Team 3, Clearwater All-Stars)
Average turns per trial	6.7	5.4
Highest turn count	13 (Trial A10)	14 (Team 9, Chlorine Kings)
Lowest turn count	3 (Trials A8, A20)	2 (Team 16, Team Backwash)
% trials/teams scoring ≥7.0 avg	25% (5 of 20)	6% (1 of 16)
% trials/teams scoring 8 at least once	85% (17 of 20)	63% (10 of 16)

Key finding: Group A's mean average score (6.5) outperformed Group B's (6.1) by 0.4 points. However, Group B produced the single highest-performing trial of either group: Team 3's perfect 8.0 average. This suggests that tool familiarity provides a more consistent baseline, but domain expertise has a higher ceiling when operators understand the exercise format.

Response Pattern Differences

The most striking differences between the two groups are qualitative, not quantitative. The technical support team and the water operators approached the same crisis from fundamentally different mental models.

Technical Support Team: Process-Oriented Responses

Group A's inputs followed a systematic crisis management framework, likely informed by their familiarity with how the scoring engine evaluates responses:

- **Formulaic first action**: Every trial used nearly identical phrasing for Turn 1 ("*Notify authorities and switch to manual operations*")
- **Abstract stakeholder management**: "*Prepare a public statement and contact legal stakeholders*"
- **Generic DFIR engagement**: "*Request assistance from a DFIR company*"
- **Meta-level closure**: "*Is there any other steps worth taking within this exercise?*"

These responses demonstrate knowledge of crisis management theory but lack operational specificity. They are the responses of someone who knows what the system rewards, not someone who has lived through facility operations.

Water Operators: Operations-Oriented Responses

Group B's inputs reveal deep operational instincts and facility-specific knowledge:

- **Physical verification:** "*Send operators into the field to verify the situation. Check readings and equipment status. Run in-hand.*" (Team 7) — "*in-hand*" is industry jargon for manual/local operation of equipment
- **Process compliance focus:** "*Take manual readings and recordings throughout the plant to verify compliance and catch any outliers.*" (Team 4) — operators instinctively prioritize permit compliance
- **Grab samples:** "*Conduct field verifications, including grab samples.*" (Team 11) — specific laboratory procedure for water quality verification
- **PLC network isolation:** "*Disconnect from the PLC network to isolate outside commands.*" (Team 9) — precise technical language from operators who work with these systems daily
- **Paper logs:** "*Ensure operators begin their rounds and begin tracking data on paper logs.*" (Team 10) — real-world fallback procedure
- **Water quality testing post-incident:** "*Conduct tests of our water in the plant to make sure that the hackers didn't change the process.*" (Team 8) — immediate concern that process parameters were tamulated
- **Cyber insurance:** "*Contact cyber insurance to ensure corrective actions will not violate policy/contract terms.*" (Team 9) — sophisticated risk management awareness
- **Cross-facility alerting:** "*Inform other facilities on network of potential breach.*" (Team 9) — awareness of interconnected utility networks
- **Alternative water supply:** "*Secure alternative supply of water as needed for the public.*" (Team 7) — public health contingency thinking
- **Incident command structure:** "*Implement an incident command team.*" (Team 4) — ICS framework from emergency management training

None of these responses appeared in any of the 20 pre-competition study trials. They represent authentic operational knowledge that cannot be replicated by tool familiarity alone. The operators responded to the crisis the way they would in real life, with actions grounded in plant operations, regulatory compliance, and public health protection.

Notable Team Performances

Team 3: Clearwater All-Stars (Avg 8.0)

The highest-performing team in either group. Their four inputs demonstrate what happens when operational expertise meets clear, decisive communication:

1. Immediate system isolation with department-wide notification and IT engagement (Score: 8)
2. Standalone backup systems, chain-of-command notification, inter-agency alerting, and public relations preparation, all in a single compound input (Score: 8)
3. Employee retraining and SOP/technology updates (Score: 8)
4. Law enforcement notification (Score: 8)

Their compound-action approach mirrors the optimization discovered in the pre-competition study but arrived at independently through operational experience. They instinctively combined multiple related actions by inputting the same technique the technical support team learned through iteration.

Team 9: Chlorine Kings (Total 94, 14 turns, Avg 6.7)

The highest total score in the event. Their 14-input sequence represents the most comprehensive incident response of either group, including actions no other team or pre-competition study trial addressed: cyber insurance verification, off-duty operator callout, cross-facility network alerting, and regulatory classification of the incident as either a "*cyber incident*" or "*cyber-attack*" for proper agency notification.

Team 7: Turbidity Titans (Total 67, 10 turns, Avg 6.7)

Notable for using precise industry terminology ("*run in-hand*"), engaging the Public Affairs Officer by title, securing alternative water supply, and even suggesting trained personnel negotiate with the attacker to gather intelligence. Their 10-turn sequence demonstrates depth of operational thinking.

Scoring Pattern Analysis

What Scores 8 in Both Groups

Inputs scoring 8 across both groups share common characteristics:

- **Compound actions**: Multiple related actions combined in a single input
- **Specificity**: Naming specific resources, departments, or procedures rather than abstract references
- **Forward planning**: Stating not just what to do now, but what comes next
- **Stakeholder breadth**: Addressing multiple communication vectors simultaneously

What Scores Poorly in Both Groups

Both groups were penalized for:

- **Passive responses**: "*OK*", "*wait for instructions*", "*continue monitoring*" (scores 0 to 4 in both groups)
- **Single-action inputs without context**: "*Disconnect from the network*" without follow-up scored 4 (Team 6) vs. 7 when combined with notification and manual switchover
- **Vague delegation**: "*Have more communication with IT support*" (Team 14, scored 5)

What the Operators Got That the Tool Experts Missed

Several operator responses revealed scoring dimensions the pre-competition study did not explore:

- **Post-incident process verification (Team 8, scored 7): Testing water quality after the incident to ensure the attacker didn't alter treatment parameters. No pre-competition study trial considered this.**
- **Regulatory incident classification (Team 9, scored 7):** Distinguishing between a "*cyber incident*" and "*cyber-attack*" for proper agency reporting. This reflects real-world regulatory awareness.
- **PII breach assessment (Team 6, scored 8): Checking whether personally identifiable information was compromised. This data privacy consideration was absent from all 20 pre-competition study trials.**

Conclusions

1. **Tool familiarity raises the floor; domain expertise raises the ceiling**.

   The technical support team achieved higher average consistency (6.5 vs. 6.1 mean of averages) through optimized phrasing and turn-count management. But the event's top team (8.0 average) outperformed every pre-competition study trial. Domain expertise, when combined with decisive communication, produces superior crisis management outcomes.

2. **Operational authenticity is a feature, not a limitation.**

   Operator responses like "*run in-hand*", "*grab samples*", "*paper logs*", and "*PLC network disconnect*" are operationally richer than the pre-competition study's generic "*switch to manual operations*". AutoTableTop™ 2.0's scoring engine correctly recognized and rewarded this specificity, demonstrating the platform's ability to evaluate domain-specific responses.

3. **The passive-response penalty is universal.**

   Both groups were penalized identically for passive inputs. "*OK*" scored 0 in the pre-competition study as well as "*wait for further instructions*" scored 0 in the event. This validates the scoring engine's consistency across user populations.

4. **Compound actions are instinctive to experienced operators.**

   The pre-competition study's key optimization, combining multiple related actions per input, was independently discovered by top-performing participating teams (particularly Teams 3, 7, 9, and 10) without any coaching. This suggests that the scoring engine's reward structure aligns naturally with how experienced crisis managers think.

5. **Operators surface action categories the tool experts never considered.**

   Cyber insurance, cross-facility alerting, PII breach assessment, regulatory incident classification, water quality post-incident testing, and alternative water supply planning all appeared exclusively in the event. These represent genuine gaps in the pre-competition study's optimized script that real-world operators naturally fill.

PII Breach Assessment is the process of determining whether Personally Identifiable Information (PII), including employee records, customer billing data, Social Security numbers, payment information, was accessed or exfiltrated during a cyber incident.

A ransomware attacker who encrypted systems may have also exfiltrated data, triggering state data breach notification laws and regulatory reporting obligations separate from the operational recovery.

6. **The platform validates domain expertise without requiring cybersecurity knowledge.**

   The scenario was calibrated for operators "*not cyber focused*", and the results confirm this design goal. Teams like the Clearwater All-Stars scored the highest marks possible by applying operational discipline - system isolation, chain-of-command notification, backup system deployment, SOP updates -without ever using cybersecurity terminology.

7. **A brief orientation would dramatically improve operator scores.**

   The mean 0.4-point gap between groups is attributable primarily to turn-count management and familiarity with how the exercise progresses. A 5-minute briefing covering the compound-action strategy and the five-phase framework would likely close this gap entirely while preserving the operators' superior operational authenticity.

Implications for AutoTableTop™ 2.0

For Product Development

The event results validate AutoTableTop™ 2.0's core value proposition: the platform produces meaningful, differentiated crisis management exercises for participants with no cybersecurity background. The scoring engine accurately distinguishes between proactive and passive responses, rewards operational specificity, and generates useful exercises from minimal configuration, all confirmed by 16 independent teams using the platform for the first time.

For Sales and Marketing

This case study provides direct evidence that water & wastewater operators, the primary target market, can immediately engage with the platform and produce authentic, high-quality exercise outcomes. Team 3's 8.0 average and Team 9's comprehensive 14-turn response are compelling proof points for sales conversations in the water sector.

For the Optimized Demo Script

The pre-competition study's 6-input demo script remains valid as a baseline but should be supplemented with operator-authentic alternative phrasings for live demonstrations with water/wastewater audiences. Specifically, "*switch to manual operations*" should be paired with the operator-native "*run in-hand*" and "*physical rounds*" language to demonstrate that the platform understands and rewards industry-specific terminology.

Appendix: Competition Input Highlights

Selected high-scoring inputs from participating teams, organized by crisis management phase. These represent operationally authentic phrasings that can supplement the pre-competition study's optimized demo script.

Phase 1: Initial Response

- **Team 3 (Score: 8):** "*I will immediately take the system offline and make sure it is not connected to the network. I will also check the other systems, notifying the department that there is a cyber security threat and that everyone needs to be hands off their equipment.*"
- **Team 7 (Score: 7):** "*Send operators into the field to verify the situation. Check readings and equipment status. Run in-hand while checking status of ransomware. Contact the Chief Plant Operator and call in additional staff.*"
- **Team 9 (Score: 7):** "*Disconnect from the PLC network to isolate outside commands.*"

Phase 2: Operational Continuity

- **Team 4 (Score: 7):** "*Implement an incident command team. Set up a duplicate HMI system for controls of the plant. Have staff refrain from turning on electronics. Servers will be isolated.*"
- **Team 10 (Score: 7):** "*Ensure operators begin their rounds and begin tracking data on paper logs, perform all lab tests and transcribe all results on hardcopies to ensure the plant maintains proper permit requirements.*"
- **Team 11 (Score: 8):** "*Get constant updates from field technicians, ensuring that we maintain plant permit standards throughout the crisis. Keep documentation as event unfolds.*"

Phase 3: Stakeholder Communication

- **Team 6 (Score: 8):** "*Verify whether or not PII has been compromised within the system. Inform the public and affected employees if PII has, indeed, been compromised.*"
- **Team 7 (Score: 8):** "*Send out notice to the public and to general authorities on potential hazards for water treatment quality. Contact the PAO - Public Affairs Officer.*"
- **Team 15 (Score: 8):** "*We have to make sure we go to social media and post about the situation and reassure the public that the situation is under control.*"

Phase 4: Advanced Response Actions

- **Team 9 (Score: 7):** "*Determine cyber incident or cyber-attack to inform proper regulatory agencies.*"
- **Team 9 (Score: 5):** "*Contact cyber insurance to ensure any corrective actions will not violate policy/contract terms.*"
- **Team 9 (Score: 8):** "*Inform other facilities on network of potential breach and to be aware of their HMI/SCADA networks.*"
- **Team 8 (Score: 7):** "*Conduct tests of our water in the plant to make sure that the hackers didn't change the process and do anything bad.*"

Phase 5: Recovery & Prevention

- **Team 10 (Score: 8):** "*Law enforcement within the 72-hour window were able to locate and reprimand the attackers. Backup recovery within internal IT went well. All tracking of log information was held to a high degree.*"
- **Team 3 (Score: 8):** "*I will also work to make sure that the employees have retraining and that our systems are updated with a new SOP and technology.*"

Revised Quick Reference Card

This revised demo script integrates the pre-competition study's optimized phrasings with operationally authentic language from participating teams. Each step provides the baseline script plus operator-native alternatives for water/wastewater audiences. Print or display this for the presenter.

AUTOTABLETOP™ 2.0 — REVISED DEMO SCRIPT (WATER/WASTEWATER RANSOMWARE)

1. ISOLATE & NOTIFY: "*Immediately take the system offline and disconnect it from the network. Notify the department that there is a cybersecurity threat and that everyone needs to be hands off their equipment. Notify IT, supervision, and the lead operator.*"

→ *Operator alternative:* *"Disconnect from the PLC network to isolate outside commands. Contact the Chief Plant Operator and call in additional staff."*

→ *Wait for facilitator narrative response*

2. OPERATIONAL CONTINUITY: "*Send operators into the field to verify the situation. Check readings and equipment status. Run in-hand. Begin tracking data on paper logs, perform all lab tests, and transcribe results on hardcopies to ensure the plant maintains proper permit requirements.*"

→ *Operator alternative:* *"Conduct field verifications, including grab samples. Take manual readings throughout the plant to verify compliance and catch any outliers."*

→ *Wait for facilitator narrative response*

3. EXPERT ENGAGEMENT: "*Does the facility have an ongoing contract with a DFIR company or cybersecurity incident response resources? Request assistance and hand them the information and access necessary to remove the threat. Contact local law enforcement and regulatory agencies.*"

→ *Operator alternative:* *"Engage external cybersecurity personnel. Review SOP for cyber security attacks. Contact water board and other regulatory agencies. Determine if this is a cyber incident or cyber-attack for proper reporting."*

→ *Wait for facilitator narrative response*

4. STAKEHOLDER COMMUNICATION: "*Prepare a public statement and contact legal stakeholders. Verify whether PII has been compromised. Send notice to the public and authorities on potential hazards for water treatment quality. Contact the Public Affairs Officer.*"

→ *Operator alternative:* *"Inform other facilities on the network of the potential breach. Go to social media to reassure the public that the water is safe. Contact cyber insurance to ensure corrective actions don't violate policy terms."*

→ *Wait for facilitator narrative response*

5. RESOLUTION & VERIFICATION: "*Continue manual/local operations until the cybersecurity team confirms the ransomware is removed. Before reintroducing the HMI and switching back to automatic operations, conduct tests of the water to make sure the attackers didn't alter treatment process parameters.*"

→ *Operator alternative:* *"Get constant updates from field technicians, ensuring we maintain plant permit standards throughout the crisis. Keep documentation as the event unfolds."*

→ *Wait for facilitator narrative response*

6. POST-INCIDENT & CLOSURE: "*Prepare a debrief and lessons learned. Update systems and SOPs. Ensure employees receive cybersecurity retraining. Analyze what allowed the breach and implement solutions to prevent recurrence.*"

→ *Operator alternative:* *"Update firewalls, add dual-factor authentication, longer passwords, and limited login attempts. Have all operators retrained on cyber awareness. Ensure backup and recovery systems are tested and validated."*

→ *System concludes exercise and generates After-Action Report*

Target: 6 inputs | 20 minutes | Scoring: 0 to 10 per turn (10 rarely awarded) | Awards: Top 3 by cumulative total score

Appendix: Competition After-Action Reports

AutoTableTop™ 2.0 generated After-Action Reports for all 16 participating teams. This appendix compares the AAR findings from the event against the pre-competition study AARs to identify how the system evaluates operationally authentic responses differently from tool-optimized responses.

Competition AAR Metrics Summary

#	Team	Coord. Score	Containment	Comms	Decisions
1	Lone Star Operators	Moderate	Successful	Moderate	15 min
2	Basin City Legends	Good	Effective	Moderate	1 hour
3	Clearwater All-Stars	High	Excellent	Moderate	Immediate
4	Headworks Heroes	Moderate	Successful	Moderate	Minutes
5	Aeration Aces	8/10	Fair (5.5/10)	6/10	4 hours
6	Floc Squad Alpha	High	Successful	Moderate	1 hour
7	Turbidity Titans	7/10	Good (6.7/10)	High	30 min
8	Grit & Grind Crew	N/A	High	Proactive	30 min
9	Chlorine Kings	8/10	7/10	High	1 hour
10	Effluent Eagles	8/10	High	Moderate	Minutes
11	Microbe Mavericks	Good	Successful	High	Swift
12	Settling Basin Squad	Moderate	Fair	Low	Delayed
13	Team Weir Gate	Moderate	Moderate	Effective	1 hour
14	Austin Pump Station Posse	Internal	Maintained	Needs work	Immediate
15	Sludge City Senders	Good	Moderate	High	Delayed
16	Team Backwash	Moderate	Partial	Limited	1 hour

AAR Quality: Competition vs. Pre-Competition Study

Comparing the AAR outputs between the two groups reveals how the report generation engine adapts to different response styles:

Containment Ratings

The event produced a wider range of containment assessments than the pre-competition study. Team 3 received "*Excellent*", a rating that appeared in none of the 20 pre-competition study AARs, where the highest was "*Successful*". At the other end, Team 5 received a precise numerical rating of "5.5/10" and Team 12 received "*Fair*" with explicit criticism that "*the overall approach was too passive, missing opportunities for swift containment*". The AAR engine's ability to clearly distinguish between Team 3's decisive response and Team 12's passive approach confirms its scoring validity across user populations.

Improvement Areas

The event AARs flagged improvement areas that are qualitatively different from the pre-competition study:

- **Pre-competition study improvement areas focused on crisis management process gaps: passive waiting, public communication timing, and transition planning.**
- **Competition improvement areas** focused on operational and technical specificity: "*initial containment strategies need refinement*" (Team 10), "*network disconnection without immediate communication alternatives*" (Team 6), "*reverting to a previous software version*" as a flawed recovery approach (Team 5, scored 3), and "*delayed determination of source and urgency by IT*" (Team 15).

The event AARs demonstrate that the AAR engine tailors its improvement feedback to the actual actions taken, not to a generic checklist. When operators took operationally specific but technically flawed actions (like shutting off the computer at the power, Team 10, scored 4), the AAR correctly identified that this "*could have resulted in data loss and was not the most sophisticated containment method*".

Successful Actions Identified

The AAR engine highlighted successful actions that reflect each group's strengths:

- **Pre-competition study successful actions emphasized process adherence: authority notification, DFIR engagement, public statement preparation, and lessons-learned documentation.**
- **Competition successful actions** emphasized operational outcomes: "maintenance of plant permit standards and documentation" (Team 11, scored 8), "operators dispatched to field for equipment status verification" (Team 7, scored 7), "verification of PII compromise" (Team 6, scored 8), "securing alternative water supplies" (Team 7, scored 8), "water tests to ensure process integrity" (Team 8, scored 7), and "alerting other facilities to potential breaches" (Team 9, scored 8).

Operational Training Insights

The competition AAR's generated richer operational insights than the pre-competition study, reflecting the operators' real-world context:

- Team 2: "*Rapid containment actions are crucial for minimizing ransomware impact. Effective manual operation ensures continuity during cyber incidents.*"
- Team 8: "*The importance of quick decision-making and manual operation capabilities in technology-dependent environments.*"
- Team 9: "*Immediate PLC disconnection was effective in threat containment. Early manual operations ensured continued water supply.*"
- Team 10: "*Importance of maintaining manual data logs during digital system failures. Effectiveness of engaging external contractors for dual-path recovery strategies.*"
- Team 11: "*Proactive public communication is crucial in maintaining trust. Cross-department coordination enhances response effectiveness.*"

These insights are grounded in facility operations experience rather than abstract crisis management theory. The AAR engine successfully extracted and articulated these domain-specific takeaways.

Safety Recommendations

The competition AAR's produced more technically specific safety recommendations than the pre-competition study:

- Team 8: "*Conduct regular water quality tests post-incident to ensure no system tampering. Implement dual-factor authentication for system access. Enforce strong password policies and limit login attempts.*"
- Team 10: "*Enhance SCADA system security by implementing regular updates and network segmentation. Develop comprehensive initial containment procedures to prevent data loss.*"
- Team 6: "*Develop alternative communication methods for use during network isolation.*"

These recommendations reflect the operators' understanding of their actual infrastructure, whereas the pre-competition study's recommendations remained at the level of "*enhance cybersecurity measures*" and "*conduct regular drills*".

MITRE ATT&CK TTP Mapping

None of the 16 event AARs triggered MITRE ATT&CK tactic identification, consistent with the pre-competition study where only 1 of 20 trials (A12) produced TTP output.

This confirms that TTP mapping requires sufficient technical depth in the participant responses to trigger, and that the beginner/basic configuration intentionally de-emphasizes technical cybersecurity detail in favor of crisis management decision-making.

Key AAR Insight

The most significant AAR insight from the event is Team 3's "Excellent" containment rating. This is the highest containment assessment produced by any trial in either group.

The AAR engine awarded this rating to a team of water operators with no cybersecurity background and no prior AutoTableTop™ experience, based purely on the quality of their crisis management decisions. Their AAR explicitly states: **"Participants demonstrated strong crisis response through decisive actions like system isolation and multi-agency coordination."**

This is the strongest possible validation that AutoTableTop™ 2.0's assessment engine accurately evaluates crisis management competence independent of cybersecurity knowledge.

Appendix: Expert Reviewers

This case study was informed by two recognized experts in water sector cybersecurity who served as subject matter reviewers and event coordinators for the water industry operations competition deployment.

Doug Short, CISM, CGCIO, GSTRT, GCCC: Trinity River Authority

Doug Short is the Chief Information Officer at Trinity River Authority of Texas (TRA), where he was hired in 2014 as TRA's first-ever CIO and CISO. TRA is a conservation and reclamation district providing water and wastewater treatment, along with recreation and reservoir facilities, for municipalities within the nearly 18,000-square-mile Trinity River basin.

Short brought 28 years of active-duty service in the United States Air Force to his role at TRA, where his military career focused on information technology and cybersecurity. His service included assignments as Chief of Staff to the Chief Information Officer and Chief of the Enterprise Architecture Branch for the US Air Force, and as Chief Operating Officer (Commander) of an Operations and Maintenance Squadron. He is a graduate of the Air Command and Staff College, the Joint and Combined Warfighting School, and the Air War College. He also graduated from the FBI's Chief Information Security Officer Academy.

Short holds a Bachelor of Science in Computer Science and a Master of Arts in Computer Resource and Information Management. His professional certifications include Certified Information Security Manager (CISM), Certified Government Chief Information Officer (CGCIO), GIAC Security Essentials (GSTRT), and GIAC Critical Controls Certification (GCCC).

Short is deeply embedded in the Texas water sector cybersecurity community: he is a member of the Texas Cybersecurity Council, chairs the Texas American Water Works Association (TAWWA) Resiliency and Cybersecurity Committee, and serves on the state water environment association Safety and Security Committee. He speaks regularly at national and local cybersecurity conferences.

Role in this study: For the 2026 water industry operations competition, Short served as the cybersecurity exhibition event coordinator - the individual responsible for integrating AutoTableTop™ 2.0 into the event framework, managing the event logistics, and overseeing the exercise execution for all 16 participating teams. His dual perspective as both a water sector CIO/CISO and Short provides unique authority on whether the platform delivers meaningful results for water/wastewater operations professionals in a competitive setting.

Randy (William) Petersen: San Jacinto River Authority

Randy Petersen is the SCADA Superintendent at San Jacinto River Authority (SJRA), where he has spent over thirteen years focused on operational technology with a strong emphasis on networking and cybersecurity. He is responsible for the collective network and server infrastructure, programming, and cybersecurity of the river authority's industrial control systems — an environment spanning over 1,200 network devices including PLCs, HMIs, SCADA servers, and field instruments across multiple divisions.

Petersen is a recognized authority in the OT cybersecurity community. He is a co-founder of the SCADA User Group, serves on the TAWWA Resiliency and Cybersecurity Committee, holds ISC2 certification, and is a frequent speaker at industry conferences including OT.SEC.CON., HOU.SEC.CON., and CYBR.SEC.CON. He has published on topics including network asset visibility, OT cybersecurity program development, and the availability-first mindset that distinguishes OT security from IT security. His NACWA publication "10 Practical Steps to Reduce SCADA Cybersecurity Risk" is widely referenced in the water sector.

Role in this study: Petersen provided the original scenario configuration for the water industry operations competition cybersecurity event and conducted an independent evaluation of AutoTableTop™ 2.0 using the event settings. His exercise transcript revealed the "*physical rounds*" response, the most operationally authentic action in the entire study, which validated the scenario's accessibility to the target audience. His minimalist configuration approach (most fields left blank) confirmed that AutoTableTop™ 2.0 generates coherent exercises from minimal input.