Southern Illinois University Carbondale
OpenSIUC

2003 Conference Proceedings

7-30-2003

Response to and Recovery and Remediation from Malicious Attacks on Water and Waste Water Utilities: a Training Curriculum for Emergency Operations Planning

Follow this and additional works at: http://opensiuc.lib.siu.edu/ucowrconfs_2003
Abstracts of presentations given on Wednesday, 30 July 2003, in session 5 of the UCOWR conference.

Recommended Citation
"Response to and Recovery and Remediation from Malicious Attacks on Water and Waste Water Utilities: a Training Curriculum for Emergency Operations Planning" (2003). *2003*. Paper 15.
http://opensiuc.lib.siu.edu/ucowrconfs_2003/15

This Article is brought to you for free and open access by the Conference Proceedings at OpenSIUC. It has been accepted for inclusion in 2003 by an authorized administrator of OpenSIUC. For more information, please contact opensiuc@lib.siu.edu.

RESPONSE TO AND RECOVERY AND REMEDIATION FROM MALICIOUS ATTACKS ON WATER AND WASTEWATER UTILITIES: A TRAINING CURRICULUM FOR EMERGENCY OPERATIONS PLANNING

Jan R. Gerston[1] and L. Keith McLeroy[2]

Jan Gerston, Science Writer.
Texas Water Resources Institute
Texas A&M University
College Station, TX 77843-2118
(979) 845-1852
jgerston@tamu.edu

Keith McLeroy, Instructor
Public Sector Training
Texas Engineering Extension Service
Texas A&M University
College Station, Texas 77843-8000
(979) 458-0912
keith.mcleroy@teexmail.tamu.edu

Water and wastewater systems are widespread networks with a myriad of possible access points vulnerable to compromise. Public water and wastewater treatment operations, therefore, must be concerned not only with implementing enhanced security measures, but also with development of strategies for detection, response, recovery, and remediation in the case of a malicious attack.

Existing emergency operations plans dealing with natural and technological disasters must be supplemented with response procedures in the case of attack by weapons of mass destruction or other malicious intrusion.

The President's Commission on Critical Infrastructure Protection (1998) identified three attributes crucial for public water supplies: (1) there must be adequate quantities of water on demand, (2) it must be delivered at sufficient pressure, (3) it must be safe to use. Actions that affect any of these factors can be debilitating for the infrastructure. Not only does the loss of potable water threaten health and commerce, but the loss of water could disable fire-fighting capability, a critical operational component of emergency response.

To address the emergency operations planning needs of public water and wastewater utilities, the Texas Engineering Extension Service (TEEX) created a series of training courses dealing with terrorism preparedness and detection and response in case of the use of weapons of mass destruction (WMD). The four courses, created under the sponsorship of the Office of Domestic Preparedness of the Department of Justice, are targeted to four levels of employees: executive, plant operations, distribution and collection, and small systems.

These courses were taught in Florida through a partnership with the Florida Counter-Terrorist Assessment Planning Committee and the National Emergency Response and Rescue Training Center in College Station from February to June 2003. Courses are then offered across the country until June 2004. Course schedule can be found at http://teexweb.tamu.edu.

Topics covered in the courses include—

- characteristics of potential chemical, biological, and radiological agents and explosives;
- delivery methods of agents;
- conduct of vulnerability assessments to determine current state of preparedness, mitigate risk, and enhance security;
- development of or revision of existing emergency response plans;
- response, remediation, and recovery;
- coordination with local emergency response organizations and health officials;
- coordination with local emergency response organizations and health officials;
- public information during and after an attack by weapons of mass destruction.

WMD are defined as destructive devices, including disease-causing organisms, incendiary devices, radioactive releases, poisonous gas, or explosives. Public water and wastewater systems are particularly vulnerable to attack because—

- The infrastructure is dispersed over a wide geographic area with multiple components (reservoirs, wells, booster stations, mains, service connections);
- Many components are accessible to intrusion;
- Increasing automation lends itself to malevolent intrusion;
- Water and wastewater systems are often considered part of "the establishment."

Module 1, Terrorism/WMD Threats to Water and Wastewater Systems teaches participants to identify common traits of terrorism: intimidating or coercing action to address political or social goals. In other words, a threat to achieve a larger agenda. While all acts of terrorism are criminal acts, not all crimes—such as opportunistic vandalism—are not terrorism. After completing this module, participants will be better able to identify threats.

Terrorism continues because it often appears to achieve its goal of effecting change for the benefit of the perpetrator's agenda. The apparent random selection of targets, weapons and timing makes terrorism very difficult to prevent. Terrorism is also cost-effective, particularly when compared with direct confrontation. It is therefore a feasible approach for asymmetric conflicts—the David-and-Goliath battle. Weapons used by terrorists can be technologically primitive, although sophisticated bioterrorism is also a threat.

Simple loss of confidence in a critical infrastructure by the public could be a terrorist goal. Frightening to the general public (and the subject of several horror movies over the past 20 years) is the threat of contamination of a basic component of life. A similar situation is suggested by the 2001 US Mail anthrax scare.

Module 2, Assessing Terrorism/WMD Risks for Water and Wastewater Systems, describes common methodologies for vulnerability assessments, teaching participants to identify and assess vulnerability of critical system components. In 2002, the Public Health Security and Bioterrorism Preparedness and Response Act required that every community water system with more than 3,300 connections conduct vulnerability assessments and revise emergency response plans. Vulnerability assessments may also be required of wastewater utilities in the future.

In general, the security assessment process for both water and wastewater involves asset characterization to determination of critical components, prioritization of adverse consequences, identification of malevolent acts and their likelihood, evaluation existing security systems, and development of a prioritized plan for risk reduction.

For potable water systems, the USEPA endorses RAM-WSM, developed by Sandia Labs in a cooperative effort between the FBI, Centers for Disease Control, American Water Works Association (AWWA), Association of Metropolitan Water Utilities, and several large utilities. The goal of the TEEX training course is to familiarize students with the RAM-WSM methodology, although certification is a three-day course offered by Sandia and private companies.

On the wastewater side, VSAT™ (Vulnerability Self-Assessment Tool), developed by the Association of Metropolitan Sewerage Agencies and two consulting companies, provides a comprehensive system for analyzing threats, as well as natural disasters.

Once a utility has assessed its risks, the goal of **Module 3, Reducing Terrorism/WMD Risks for Water and Wastewater Systems,** is to lead participants through the process of determining safeguards or mitigation measures. Although it is not possible to eliminate risk entirely, the utility must determine an acceptable level of risk. A determined adversary with proper equipment can overcome any security system eventually.

Physical security systems delay access, detect an incident of unauthorized access, and respond by alerting proper authorities. Passive physical security measures include access control, lighting, perimeter security, and interior detection system. Active security measures include security patrols, controlled access, with employee instructions to question strangers, cancellation of treatment facility tours, and restricted public access to reservoirs.

Since physical protection systems will only delay a malevolent entry, it is advisable for utilities to emphasize operational safeguards. It is much more cost-effective for an operational change to reduce the severity of the consequence rather than installing security features to prevent intrusion.

On the operational side, redundancy of raw water sources or interconnection supply agreements could provide a water source in emergencies. Maintenance of an adequate chlorine residual, backflow prevention, and maintenance of up-to-date system plans for isolating trouble areas can also lessen consequences.

On-line water monitoring systems can be installed to detect changes in physical, chemical or biological characteristics. Continuous monitoring of chlorine residuals can be supplemented with biosensors, including commercially available bivalve sensors—mussels with close in response to chemical contaminants.

Often overlooked is the importance of community awareness, both within the utility's own corporate culture and outside vigilant "watchdogs" in rural areas.

Automated control systems could be a target of remote intrusion. Many SCADA systems are susceptible to hacking, lax password setting, viruses, and vendor manipulation.

Since physical protective systems and operational measures cannot protect against any and all malevolent intrusions, utilities must plan a response to malevolent intrusion, the topic addressed in **Module 3, Responding to Terrorism/WMD Incidents**. Terrorism incidents may not be recognizable until the incidence of multiple casualties, and even then victims and first responders may inadvertently carry an agent into another public place. Support facilities, local emergency responders, and 911 centers may be overwhelmed.

The Association of Metropolitan Water Utilities and the National Infrastructure Protection Center spearheaded the establishment of the Internet-based Information Sharing and Analysis Center (ISAC). ISAC is a secure forum for member agencies to share information on malicious water and wastewater incidents, with the goal of predicting trends and providing timely warnings to water and wastewater utilities.

The Water Protection Task Force, established by the USEPA in October 2001, published *Guidance for water Utility Response, Recovery & Remediation actions for Man-made and/or Technological Emergencies* to inventory minimum level of actions to be taken by an affected utility. Using the framework of this document, course Modules 4 and 5 cover responding to and recovering from terrorism/WMD acts: notification of health officials, the media, and customers; response actions to be taken at source water, treatment facilities, distribution and storage, wastewater collection; and wastewater treatment facilities; response to SCADA intrusion; response to plant damage.

Once an incident has been confirmed, public reaction will be stronger than for emergency incidents caused by natural disasters. The public, as well as emergency responders, has a right to know about hazardous situations, mandated by the Emergency Planning and Community Right-to-Know Act. Communicating a threat proactively through the media establishes credibility, allows the utility to control the accuracy of information, builds public trust, and allows meaningful public involvement.

The ultimate goal of effective crisis communication, of course, is to save lives and protect public health. Utilities must communicate in a manner that engenders trust and confidence. AWWA recommends the utility be the first to deliver the bad news. Early release of information sets the pace for resolution of the problem. People are entitled to information that affects their lives.

Dry runs of the emergency response plan should include practice of the communications portion of the plan.

Although it is impossible to protect a utility against any conceivable risk, by assessing critical components and assumed risk, hardening physical security and operational measures, and effectively keeping staff current on emergency response plans, water and wastewater utility managers can mitigate both the risk and the damage to their infrastructures.

REFERENCES

DeNileon, Gay Porter, 2001. The Who, What, Why, and How of Counterterrorism Issues, *Journal of the American Water Works Association,* 93(5): 78-85

Gerston, Jan, 2002, *Water and wastewater utilities enhance system security: Malicious attacks now to be addressed along with natural disasters in new plans.* Texas Water Resources, December 27, v. 27, n.2

Planning for and Responding to Terrorism/Weapons of Mass Destruction (WMD) Incidents in Drinking Water and Wastewater Utilities: Participant Manual. 2002. US Department of Justice, Office of Domestic Preparedness and Texas Engineering Extension Service, College Station, Texas.

Ruckman, Kathryn, 2002. Drinking Water Research: A Update from the AWWA Research Foundation, 12(5) 2-5.

Wettering, Larry, 2002. Lessons Learned: Taking Security into the Next Level, *Opflow*, American Water Works Association, 28(2) 8-10.