Texas Water Resources Institute

Texas Water Resources

December 2002
Volume 27
No. 2

Water and Wastewater Utilities Enhance System Security

Malicious attacks now to be addressed along with natural disasters in new plans

by Jan Gerston, Texas Water Resources Institute

The mission of America's water utilties is to provide safe and sufficient water and wastewater treatment to customers. Historically, the big issues in water safety were microorganisms, disinfectant by-products, and infrastructure maintenance. Long before the tragic events of 9/11, however, water utility managers, law enforcement agencies, local emergency planning committees, and epidemiologists were laying the groundwork for averting, detecting, and responding to other threats. Those efforts, however, were directed at low-level threats such as burglary, vandalism or natural disasters. Understandably, the events of 9/11 triggered a new perspective on water system security. Since the terrorist attacks, security measures have been examined, revamped, and redoubled in every facet of the nation's utility infrastructure.

Detect, delay, respond

The mission of any security system is to detect, delay, and respond to destructive action. Destructive action to a water system could range from vandalism, such as members of the senior class painting their class year on the water tower and dumping the paint can into the tank, to cyber sabotage by a disgruntled insider, all the way to a full-fledged terrorist attack on a major treatment plant.

By their nature, utility systems are inherently difficult to secure. The physical assets are ubiquitous and the distribution systems accessible. Whereas a building is a single physical structure, a water system is a widespread network with a myriad of possible access points vulnerable to compromise. Also, most older plants were built without security as a priority.

An attack on a water system does not require high-tech tools, well-organized teams, or exotic chemicals. For instance, in Neenah, Wisconsin, a group of teenagers gained access to a water treatment plant with a stolen key. They planned to string trip wires, spread liquid soap on the floors, contaminate filters with dry soap powder, and ignite firecrackers near chemical tanks. The youths were armed with baseball bats, dressed in dark clothing, and carried radios and flashlights. Fortunately the plan was thwarted when a would-be accomplice alerted police. (Wettering, February 2002)

Equally important to the operation of a water system as its capital assets are the external supporting infrastructure—energy, transportation, and telecommunications. Effective security measures must protect all the members of this interdependent web of operations from physical destruction, contamination, and cyber attack.

Security is built from a combination of policies, procedures, people, and technology, according to Jeffrey Danneels, Manager of the Security Systems and Technology Center at Sandia National Laboratories in New Mexico. Policies must be developed to address risks and communicated with employees. Operating procedures must be modified to meet policy goals. And although every employee must be cognizant and compliant with security procedures, security system monitoring cannot be loaded as collateral duties onto already burdened operators.

Elements of a water system vulnerable to attack

A water system consists of its sources, treatment facilities, controllers, distribution and storage system, and wastewater treatment. According to Danneels, "To protect one component of the system and neglect the protection of others will not achieve the objective of improving the security within the water infrastructure" (Danneels, 2001).

One-ton gas cylinders contain chlorine used to disinfect drinking water poses a respiratory and skin blister hazard.

Raw water sources

Contamination of large-volume water supplies, such as reservoirs, is considered unlikely as it is difficult to obtain and transport sufficient quantities of hazardous materials to contaminate sources. As water volume decreases, the risk of contamination increases (Danneels, 2001). Conventional water treatment technologies are effective in removing most biological agents, assuming the water treatment process has not been compromised. However, treatment methods may not deter all contaminants, especially as chemicals and pharmaceuticals.

Early warning systems with real-time monitoring sensors are needed to protect against and to warn of contamination of raw water sources. To rely on after-the-fact reporting by the medical community of illnesses is not an effective method of detection.

An effective early warning system would alert operators in time to take action, be expandable, allow remote operation, require low skill to operate, give minimal false reports, and be verifiable.

Water treatment plants

Potable water treatment plants employ an array of chemicals, most notably chlorine, that could be used to cause harm to the surrounding community with a deliberate release, or to contaminate the water supply by increasing chemical injection rates to dangerous levels.

The integrity of the plant could be breached by perpetrators climbing over or burrowing under fences, avoiding infrared sensors and nullifying alarms. Access can be as simple as a stolen key, as in Neenah, Wisconsin, or a leaked access code. A disgruntled employee could be recruited to sabotage a plant. Often contractors have easy access.

Chemicals used in water treatment should be kept in a secure area.

In recognition of these vulnerabilities, some water utilities are requiring escorts for contractor technicians who need access to sensitive areas, keeping tighter rein on keys and access codes, and changing passwords on a regular basis.

Control systems

Also at risk are supervisory control and data acquisition (SCADA) systems used to automate almost all modern water and wastewater treatment plants. Often passwords on control equipment are not changed from the default. Many SCADA systems are susceptible to hacking, which could result in disclosure or theft of information, corruption of data, or denial of service. Because many SCADA systems are not connected to the Internet, the threat of cyber attack is considered most likely from an employee with access (DeNileon, 2001).

Distribution systems

Of the three elements of a drinking water system—source water, treatment plant, and distribution system—the distribution system of pipelines, pumps, and storage tanks offers the greatest opportunity for malicious action because it is extensive, relatively unprotected and accessible, and often isolated.

Wastewater treatment

If potable water is compromised, it is only a matter of time before wastewater is affected. In the event of contamination, wastewater treatment plants would have to be shut down to avoid contamination of the receiving stream. Also, the wastewater treatment plant itself could be the target of a physical attack.

Threats

The threats to a water or wastewater system are broadly classified into physical destruction, bioterrorism and chemical contamination, and cyber attack.

Physical destruction of a water system's assets or disruption of the water supply is considered more likely than contamination. Explosives and guns are more easily obtained than large quantities of harmful chemicals. Instructions for fabricating explosives are posted in the Internet. An attack on a treatment plant can be accomplished by a small group with a minimum of organization.

A loss of water pressure would compromise firefighting capabilities and also lead to possible bacterial build-up in mains and pipes. Another concern is the potential for creating a system-wide water hammer effect by opening and closing major controls valves too quickly, resulting in a simultaneous main breaks. (DeNileon, 2001)

More frightening to the general public (and the subject of several horror movies over the past 20 years) is the spectre of contaminants introduced into the drinking water supply.

Even the chemicals used by utilities to treat water could be a hazard. Chlorine is a potentially lethal respiratory hazard. The delivery chain also presents a vulnerability. Smaller utilities receive chlorine, for instance, in tanks as either liquid or pressurized gas. Karl Goldapp of College Station Utilities emphasized the importance of certifying the legitimacy of delivery person, as liquid chlorine could easily be partially drained off and replaced with a noxious chemical that would be added to potable water unintentionally by the operator.

Not only pranksters, malcontents, and terrorists, but contractors and communications systems could sabotage a treatment works. The burgeoning demand for cell phones and pagers, television and radio transmission, and law enforcement communications has given rise to water towers bristling with antennas. For years, the mounting of communications antennas on water tanks was considered a win-win situation. Water utilities recouped the capital cost of towers from rent, and communication companies were relieved of the tasks of tower construction, zoning hearings, and other maintenance costs. Providing access to this communication equipment exposes the utility to potential sabotage.

In Australia, a contractor employee who installed a computerized wastewater control system, irate about being turned down later for a job with the utility, hacked into the its network, releasing raw sewage 46 times before being caught.

Protection of critical infrastructures

The President's Commission on Critical Infrastructure Protection (PCCIP), established in 1996 by President Bill Clinton, examined the security of the nation's critical infrastructures, defined as structures, information, and cyber resources essential to the minimum operations of the economy and government. The PCCIP determined that water infrastructure is highly vulnerable to a range of potential attacks. In 2000, the PCCIP convened a public-private partnership called the Water Sector Critical Infrastructure Advisory Group which helps Sandia National Laboratories in developing security risk assessment methodology.

Critical water infrastructures—the systems used to collect, treat, and distribute potable water and treat wastewater—are fundamental to the public health and welfare and are subject to both natural disaster as well as intentional attacks. Potable water is one

of the top priorities in emergency medical services, firefighting, sanitation, and general disaster recovery.

In 1998, responsibility for the critical water infrastructure was assigned to the US Environmental Protection Agency (EPA) under Presidential Directive 63, a National Security Council directive.

Vulnerability assessments

President George Bush signed HR 3448—the Public Health and Bioterrorism Response Act—on June 12, 2002. The Act amends the Safe Drinking Water Act to require that every community water system serving a population greater than 3,300 "conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable source of drinking water."

The Act authorizes $160 million in 2002 and additional funds through 2005 for drinking water utilities to conduct mandatory vulnerability assessments, revise emergency response plans, and make security upgrades. Through the EPA, both large public and private utilities—serving more than 100,000 people—are eligible for grants of up to $115,000.

In January 2002, President George W. Bush signed the FY02 Supplemental Defense Appropriations Bill directing $89 million to EPA for security-related needs. Of this amount, $53 million was earmarked for vulnerability assessments, emergency response plans, and security planning at utilities serving more than 100,000 persons or treating more than 15 million gallons per day (mgd) of wastewater. About $23 million went to security measures at smaller drinking water systems.

A compilation of water infrastructure security website links and tools can be found at http://www.epa.gov/safewater/security/index.html.

Development of a water system security framework is the responsibility of Sandia National Laboratories in New Mexico. Sandia has a proven history of developing security protocols for the nuclear weapons industry, for Department of Defense entities, and more recently, for hydroelectric dams. After reviewing the operations of a large water utility relying upon both groundwater and surface water, Sandia personnel determined that the existing Sandia risk assessment methodology could be adapted to the water infrastructure

Sandia conducted a workshop in November 2000 to develop a framework for risk assessment methodologies. Workshop participants included the Federal Bureau of Investigation (FBI), the American Water Works Association (AWWA), the Association of Metropolitan Water Agencies, and several large water utilities.

The development of the Risk Assessment Methodology for Water Utilities (abbreviated RAM-WSM), was a cooperative effort between FBI, Centers for Disease Control, AWWA, Association of Metropolitan Water Agencies, and several large utilities. As part of the development process, RAM-WSM has been tested at several larger municipal water utilities.

In an effort to disseminate the methodology widely, Sandia conducted a train-the-trainer course for consulting firms, nonprofit organizations, and water trade groups selected in a competitive process. These entities are licensed to offer the class to large utilities. A list of approved course providers can be found at http://www.epa.gov/safewater/security.

Drinking water utilities serving more than 100,000 must complete vulnerability assessments by Dec. 31, 2002, while smaller utilities have a extended deadlines (50,000 to 99,999 Dec. 31, 2003; 3,301 to 49,000, June 30,2004).

EPA's Water Protection Task Force targets the critical needs of small- and medium-sized systems, providing guidance, training, and financial assistance for conduct of vulnerability assessments, for preparation of emergency response plans, and for establishment of security objectives. The Task Force draws upon the experience of Sandia National Laboratories, and provides baseline information on potential threats.

For these smaller utilities, EPA will depend upon states, through which grants are channeled, to build upon existing partnerships with other stakeholder organizations, such as emergency response councils and community health entities, and to coordinate implementation tasks. To facilitate planning, EPA will provide support to improve communication between states and smaller water utilities.

For wastewater utilities, the Vulnerability Self-Assessment Tool (VSAT™) developed by Association of Metropolitan Sewerage Agencies and two consulting companies—PA Consulting Group and SCIENTECH, Inc.—provides a comprehensive system for analysis of both intentional threats and natural disasters. VSAT™ is available free of charge to wastewater utilities. More information can be obtained at http://www.vsatusers.net and http://www.wef.org.

Education and training

The AWWA is hosting an online water security course titled "Security Planning for Drinking Water Systems: An Operational Approach." The course is designed to help water professionals evaluate and prepare appropriate security measures in the water industry. Hypothetical hazardous situations are addressed, and step-by-step checklists are offered to keep industries, and their customers, safe from possible harm.

AWWA hosted a webcast in May entitled, *Emergency Response Planning: Counter Terrorism and Security in the Industry*. The presentations emphasizd identifying resources available to support utilities' security efforts. The Power Point presentations shown during the webcast are available at http://www.greenworks.tv/events/awwawebcast.htm.

The AWWA Research Foundation (AwwaRF) presented a satellite teleconference program on security risk assessment for drinking water utilities in November 2001 which addressed key security design principles, available security technologies, a methodology for security risk assessment at water utilities, and the process of selecting security consultants. See http://www.greenworks.tv/events/watersecuritywebcast112701.htm

On the wastewater side, the American Public Works Association, in partnership with the Water Environment Federation, the trade association of the wastewater industry, presented a webcast addressing the basics of VSAT™, security planning, and a cost benefit analysis entitled *Wastewater Security Training: Reducing Vulnerability to Both Intentional Threats and Natural Disaster* in November 2002.

The Water Environment Federation (http://www.wef.org) provides technical assistance for larger utilities: twelve two-day workshops with representatives of publicly owned treatment works treating upwards of 15 mgd on vulnerability assessment, emergency plan development, upgrade, and implementation needs. Two web-based training sessions cosponsored by the Water Envi-

ronment Federation (WEF) and American Public Works Association will summarize general security principles, introduce the VSAT™ software, and raise awareness of EPA's emergency response and recovery guide.

The AWWA Water Security Congress, March 23–26, 2003, will give utility managers and security staff training on water quality monitoring, legal and legislative issues, distribution and collection system security, source water security, crisis decision-making, crisis communications, and cyber security. See http://www.awwa.org.

On June 27, 2003, AWWA offers a webcast, *The Bioterrorism Preparedness Bill: What's Next?* to cover compliance regulations, resources available from the EPA, and working with state and local emergency planning agencies.

Risk Assessment Methodology

The new methodology represents a sea change in focus on water system security. Instead of simply assessing fences, guards, cameras, motion detectors and the like, it became important to understand and inventory threats; and identify, and prioritize critical assets and their protection. (Ruckman, 2002). A vulnerability assessment must review the entire water system—

- pipes, conveyances, and physical barriers
- water collection, pretreatment, treatment
- storage and distribution
- automated systems
- chemical handling and storage.

The new methodology puts emphasis on adequate emergency management and response to deployment of a weapon of mass destruction. The elements of an effective vulnerability analysis are—

- Formulation of a clear statement of performance requirements of a security system.
- Threat analysis of the likelihood of various adversaries attacking the utility.
- Identification of critical assets and the consequences of losing those assets.
- Identification of a spectrum of threats that can reasonably be defeated.
- Examination of all potential ways for the adversary to access critical assets.

A washout under a perimeter fence could present a security hazard at a water or wastewater treatment plant.

Information Sharing

In response to Presidential Directive 63, the Association of Metropolitan Water Agencies and the National Infrastructure Protection Center are spearheading the establishment of an Information Sharing and Analysis Center (ISAC) for the water industry. The prototype of this system is an e-mail tree that provides EPA alerts and notices to utilities. Member agencies of the ISAC will share information on malicious water and wastewater incidents with the goal of predicting trends and providing timely warnings to utilities. Information will be anonymous to protect utilities from litigation or damage to their reputations, but authenticated.

Of particular interest to utilities will be the lessons learned. It is expected that sharing of information will bring to light potential vulnerabilities and innovative solutions.

Using secure communications, the ISAC will convey threat warnings and other security issues to member utilities.

Response, recovery, and remediation

Emergency response planning is primarily a local responsibility. Every water utility should have in place an emergency response plan coordinated with federal, state, and local emergency response organizations, regulatory authorities, and local government officials. EPA recommends that utilities augment an established emergency operations plan addressing natural disasters with procedures for responding to intentional attacks. According to the EPA, counter-terrorism planning is an extension of existing activities.

Response refers to actions immediately following the incident. Recovery involves bringing the system back into operation, and remediation refers to long-term restorative action.

Of primary concern in an emergency response plan is the identification of the organizational structure responsible for incident response and management. To avoid confusion, utilities must coordinate with other emergency response activities to develop clear protocols and chains-of-command for decision-making and for reporting and responding to threats.

Entities to be alerted include emergency management personnel, law enforcement, public health officials, emergency medical services, state environmental agencies, critical care facilities, and the FBI. Contact lists of all relevant personnel should be kept current.

As with water providers, local emergency planning committees (LEPCs), established under the Emergency Planning and Community Right-to-Know Act (EPCRA), prepare and maintain comprehensive emergency plans for releases of hazardous substances. The same planning principles followed for accidental releases can be adapted to deliberate releases by terrorists. LEPC membership includes state and local officials; police, fire, civil defense, public health, environmental, hospital, and transportation officials; and representatives of facilities where chemical are stored.

The public, as well as emergency responders, has a right to know about hazardous situations. Under the EPCRA, people are entitled to information that affects their lives. Communicating a threat proactively to the public through the media establishes credibility, allows the utility to control the accuracy of information, builds public trust, and allows meaningful public involvement.

The EPA's "Guidance for Water Utility Response, Recovery, & Remediation Actions for Man-Made and/or Technological Emergencies" is available at http://www.epa.gov/safewater/security/er-guidance.pdf.

Texas efforts

Texas Section, AWWA

The Texas Section of the AWWA, under the leadership of executive director Mike Howe, pulled together a satellite teleconference, "Defending Your Utility in a National Crisis," on water systems security on November 9, 2001 with a panel including representatives of the Texas Natural Resources Conservation Commission (now Texas Commission on Environmental Quality) Public Drinking Water Section EPA Region 6, as well as Danneels from Sandia Labs. Water professionals at twelve sites in Texas participated.

Shortly thereafter, AwwaRF broadcast a satellite teleconference with a similar format, *Security Risk Assessment for Water Utilities*, featuring an introductory address by EPA Administrator Christine Todd Whitman and again, Danneels of Sandia National Laboratories.

In response to a request from EPA Region 6 and the Public Drinking Water Section of the Texas Commission on Environmental Quality, after its successful teleconference in November, Texas AWWA presented *Hardening Targets*, a program of particular interest to small- and medium-sized utilities. A videotaped segment showed a response to a staged emergency event at a rural treatment plant intended to acquaint water professionals with law enforcement and firefighter emergency procedures. A vulnerability expert called attention to security shortfalls at suburban and semirural sites.

Texas Engineering Extension Service

Funded by the US Department of Justice Office of Domestic Preparedness, the Environmental Water and Wastewater Training Program of the Texas Engineering Extension Service (TEEX) is creating four courses on preparing for, responding to, and recovering from a terrorism or weapons of mass destruction incident for water and wastewater personnel. The couses will be offered to executives, plant operators, distribution and collection personnel, and small systems (less than 250 connections) operators. As information becomes available, it will be posted at http://teexweb.tamu.edu.

The courses will cover—

- characteristics and use of potential chemical, biological, and radiological agents, explosives, and their delivery methods
- vulnerability assessments to determine current state of preparedness, to mitigate risk, and to enhance security
- development or revision of applicable emergency response plans
- responding to and recovering from incidents
- effective public interaction during and after a weapons of mass destruction/terrorism incident.

At the request of water officials in Florida, the first courses will be offered in that state from February to June 2003. Classes will then be offered across the country, including Texas, through June 2004. The course schedule will be posted on http://teexweb.tamu.edu or contact Paul Muraca or Richard Harbuck at eupwti@teexmail.tamu.edu.

The courses are hosted by the National Emergency Response and Rescue Training Center based in College Station. The Center is a member of the National Domestic Preparedness Consortium, and has developed courses to support curricula to improve the ability of public works professionals to combat terrorism.

Research Needs

At a May 2002 workshop arranged by AwwaRF, security experts identified research needs and priorities. Based upon the findings of the workshop, the AwwaRF Board of Trustees approved five research projects—

- Utility-relevant information on candidate contaminants for purposeful water-supply contamination, which will be developed into a central controlled-access database.
- Vulnerability assessment template for medium and small systems
- Extraction methods for biological agents, which will screen and test for the best method of extraction on actual bioterrorism agents.
- Assessment of capabilities of existing monitoring equipment to function as early warning/real-time systems technologies.
- Inventory of lessons learned from vulnerability assessments created for HB 3448.

The AwwaRF will continue to focus research efforts in the evolving field of security-related research. Four security-related problems under discussion are—

- Further testing and evaluation of a distribution system contaminant model developed by EPA and the Federal Emergency Management Agency and used at the 2002 Winter Olympic Games in Salt Lake City.
- Examination of household point-of-use devices as tools to help identify drinking water contamination incidents, in partnership with the Centers for Disease Control
- Development of a primer on security best management practices.
- Examination of the applications of unconventional water provision options.

To help prioritize research, the AwwaRF organized a security research steering committee composed of water community representatives t recommend a security research agenda for 2003 to the AwwaRF Research Advisory Council. In turn, the Council will suggest a 2003 research agenda to the Board of Trustees in January.

A second AwwaRF subcommittee is developing policies and procedures for handling publications with potentially sensitive security information. The charge of this group is to find the balance point between ensuring important information is available where it is needed and keeping that information from falling into the wrong hands.

The EPA works with the Centers for Disease Control and Prevention, the Food and Drug Administration, FBI, and the Department of Defense to develop information for the Homeland Security Office on biological, chemical, and radiological contamination, and how to respond to their presence in drinking water. The research will ramp-up knowledge of contaminant detection, monitoring protocols and techniques, and treatment effectiveness.

In May, the Texas A&M Board of Regents approved establishment of the Integrative Center for Homeland Security (ICHS) to serve as an umbrella organization for research into security issues of biohazards, agriculture, transportation, ports and waterways, health issues, and information archiving and security. In November the US Congress approved the Homeland Security bill, including authorization for a center at Texas A&M University.

A land-grant, sea-grant, and space-grant institution, Texas A&M University is in a unique position to assemble the research expertise required by the ICHS. The Center will take advantage of existing expertise; for instance, the Texas Transportation Institute for ports and waterways and surface transportation; and the College of Engineering for pipeline security and information security.

A related center, The Institute for Countermeasures Against Agricultural Bioterrorism, has recently been established at Texas A&M University to improve strategies for preventing and responding to attacks on the nation's agriculture system, including diagnostic systems for early detection of disease.

Texas Water Resources

IS PUBLISHED QUARTERLY BY
THE TEXAS WATER RESOURCES INSTITUTE
C. ALLAN JONES, DIRECTOR
B. L. HARRIS, ASSOCIATE DIRECTOR
RIC JENSEN, EDITOR AND COMMUNICATIONS MANAGER
JAN GERSTON, SCIENCE WRITER
ROSEMARY PAYTON AND ELLEN WEICHERT, ADMINISTRATIVE ASSISTANTS

TWRI is supported by funds provided in part by the US Geological Survey, US Department of the Interior, as authorized by the Water Resources Research Act of 1984. Subscriptions are available free upon request.

TWRI, 979-845-1851; fax, 979-845-8554; Ric Jensen, 979-845-8571; e-mail: twri@tamu.edu; http://twri.tamu.edu.

References

Blomgren, Paul "Utility managers need to protect water systems from "cyberterrorism," *U.S. Water News*, 19:10, October 2002.

Danneels, Jeffrey J., Department Manager, Security Systems and Technology Center, Sandia National Laboratories (to the US House of Representatives Committee on Transportation and Infrastructure Subcommittee on Water Resources and the Environment, "Terrorism: Are America's Water Resources and Environment at Risk?", October 10, 2001.

DeNileon, Gay Porter, "The Who, What, Why, and How of Counterterrorism Issues," J*ournal American Water Works Association*, 93:5, May 2001, 78-85.

Huntley, Gary M., Grabowski, Peter J., Pinsky, David E., "Performing a Vulnerability Assessment," *Opflow*, 27:12:13, , American Water Works Association, December 2001.

*Journal American Water Works Associatio*n, "Keeping Your Utility Safe," 94:1:31, January 2002.

Journal American Water Works Association, "Leading in a Crisis," 94:1:32, January 2002.

Peralta, Steve, " Long-term Plan Key to Emergency Response," *Opflow*, 25:11, American Water Works Association, November 1999.

Ruckman, Kathryn, *Drinking Water Research: An Update from the AWWA Research Foundation*, 12:5:2, American Water Works Foundation Research Foundation, September/October 2002.

"Technology solutions for physical plant security," Journal American Water Works Association, 94:2, February 2002, 46-48.

US Environmental Protection Agency, *Guidance for Water Utility Response, Recovery & Remediation Actions for Man-made and/or Technological Emergencies*, Office of Water Protection, April 15, 2002.

Wetterinng, Larry, "Lessons Learned: Taking Security to the Next Level," *Opflow*, 28:2:8, American Water Works Association, February 2002.

Yarlot, Nelson, "Tank-Mounted Antennas Signal Concern," *Opflow*, 26:8:3, American Water Works Association, August 2000.

Texas Water Resources Institute
TAMU 2118
Texas A&M University
College Station, Texas 77843-2118

ADDRESS CORRECTION REQUESTED

NON-PROFIT ORG.
U.S. POSTAGE PAID
COLLEGE STATION, TEXAS
PERMIT NO. 215