Utility Protection

Frank Pisciotta is a Certified Security Consultant and president of Business Protection Specialists in New York. He is also a member of the Institute of Internal Auditors and earned his Certified Protection Professional designation in 1994.

Re-evaluating Security

Did Your Risk Assessment Really Safeguard Your Utility?

Some utilities took minimal or inadequate action after completing their vulnerability assessments, which left them at risk.

BY FRANK PISCIOTTA

IN MARCH 2006, teenage vandals illegally entered a 1.3 mil gal water tank in Blackstone, Mass. A 5-gal container with a distinctive odor was found on top of the tank. Authorities ultimately determined the water wasn't contaminated, but the teenagers had successfully defeated the utility's security system by cutting the fence and disabling an alarm system. An April 2006 citywide municipal risk assessment revealed a significant exposure to water contamination that was overlooked during the initial vulnerability assessment (VA), conducted in-house in compliance with the requirements of the Bioterrorism Preparedness and Response Act of 2002.

The city administrators were dismayed to learn of such blatant exposure to contamination, and they aren't alone; other municipalities are likely operating under a similar false sense of security. Of the numerous vulnerability assessment tools used by community water system managers, none provided

- specific localized threats against which a community water system must protect itself and its consumers, or
- specific security solutions for any identified vulnerabilities.

The tools ranged from complex methodologies to simple self-assessment checklists that could be completed in minutes. Many smaller water systems chose to complete the latter, often without the assistance of a qualified security expert. This risky endeavor happened routinely, contrary to the directive in the self-assessment checklists, which state "This document is meant to encourage smaller systems to review their system vulnerabilities, but it may not take the place of a comprehensive review by security experts."

The March 2005 Government Accountability Office report "Protection of Chemical and Water Infrastructure" concludes that many water systems operate in a climate in which it is a struggle to fund security improvements. Consumers oppose rate increases, opinions differ regarding the need for security at community water systems (many feel "it won't happen here"), and employee cultures that embrace security are difficult to achieve.

Common weaknesses of completed VAs include

- incomplete and inaccurate conclusions on the quality of existing security measures;
- missed vulnerabilities that could be exploited by vandals, criminals, disgruntled former employees, or terrorists; and
- security solutions that are unimplemented, inadequate, or unreasonable.

REASSESSING THE VA

As with the incident in Blackstone, security weaknesses may become evident only after a security incident occurs or the VA is reassessed by properly trained participants. Several municipal water system case studies underscore the potential exposure to drinking water everywhere.

Checklist weaknesses and the potential for inaccurate conclusions. When one small drinking water system that relied on a free VA with a self-assessment checklist completed the list during a departmental meeting, staff considered themselves performing satisfactorily in terms of the utility's "Key control and accountability policy." However, later investigation revealed

- the utility was using low-grade keys that could be duplicated without authorization at any local hardware store;
- the utility had no tracking or accountability system to track how many keys were in circulation or where all assigned keys were at any given point;
- employees and contractors routinely separated from the company without returning keys;
- master keys were issued to senior employees who really didn't need them, and one manager had lost the key three times without a single lock being changed; and
- third-party contractors had their own locks on utility gates, and utility staff had no idea how many people the contractor had given access to utility sites.

A well-secured facility will take numerous approaches to hinder access.
USE CALL BOX TO REQUEST ENTRY
KEEP OUT
AUTHORIZED PERSONNEL ONLY
WARNING
TAMPERING WITH THIS FACILITY IS A FEDERAL OFFENSE
US CODE TITLE 42 SECT 3001-1

PHOTOGRAPH: MELANIE SCHIFF, AWWA

The self-assessment checklist question as written left a significant exposure to an invalid conclusion. For example, the checklist doesn't provide preferred alternatives to standard practice, such as the use of a controlled keyway that minimizes unauthorized duplication of keys. Mechanical locks on critical facilities should be a baseline requirement. At least 10 procedures need to be evaluated to determine the adequacy of a lock and key control program, including whether

- the tracking system is sufficient;
- keys are properly and uniquely engraved;
- locks are changed when keys are lost or stolen;
- responsibility for the management of the key control program has been assigned to a properly trained individual;
- a procedure is in place for users to sign for keys on removal and return;
- a procedure ensures the distribution of keys is appropriate, particularly for master keys;
- spare keys are controlled by a level of security that is commensurate with the value of the assets protected by the locks; and
- procedures ensure that keys are recovered when personnel separate.

So, although a checklist approach can be quick, easy, and inexpensive to execute, it often leaves a lot to be desired in terms of thoroughness and reliability of the conclusions.

Unknown vulnerability. A recent risk assessment for a municipal government, whose water department serves approximately 50,000 citizens, revealed significant vulnerabilities associated with booster pump stations. The stations featured low walls (5 ft at the highest point), unsecured chlorination injection equipment, and easily opened access ways to equipment and piping, making for easy introduction of

None of the installed alarms were being monitored. A breach of security would have gone undetected until employees returned to work in the targeted facility.

BEING READY—THE "READINESS CONTINUUM"

Being ready is really a continuum through which you and your organization will move. To pronounce ourselves truly ready to respond to the security needs of our customers and citizens, we must move through four distinct stages.

STAGE 1: UNCONSCIOUS INCOMPETENCE

With all that's occurred and all that we've experienced in the past decade or so, there are few, if any, public entities that fall into this category. At this stage, the organization is incompetent with regard to being ready to respond to extraordinary situations, but does not know it. Unless an organization has spent the past decade on the far side of Mars, it is doubtful that it will find itself here.

STAGE 2: CONSCIOUS INCOMPETENCE

In this stage, the organization has recognized the fact that its readiness capability is not competent or ready to meet the risks, hazards, and exposures your organization may face.

If your organization doesn't move on to stage 3, it opens itself to extreme liability. This liability extends not only to the organization itself, but also to its public officials and employees. As the old saying goes, "Anybody can sue anybody. The question is, can you win?" Why improve the odds of someone winning a lawsuit against you because you failed to protect your organization and customers against potential risks that you've identified?

This stage requires brainstorming and identifying risks or exposures. It also acknowledges shortfalls in mitigation, response, or recovery plans. This process will often identify an exposure for which you haven't planned at all. Many organizations will find that their existing plans to respond to potential extraordinary events are inadequate. This is quite normal. It isn't shameful to find yourself in stage 2. Remaining there, however, is derelict in your duty. The key is to take action, and take it quickly. A first step in stage 2 can be to conduct a simple evaluation of the current working environment within which your organization operates.

STAGE 3: CONSCIOUS COMPETENCE

In this stage, you'll be expanding your visioning and planning activities. You'll develop a plan and conduct training, both to raise the competence of your staff and to test the plan. Even though an organization at this stage will effectively handle most extraordinary events, that success will not be gained without some costs. Errors will still be made, inefficiencies will degrade performance, and the organization will not yet function at its maximum capability. But if you maintain your focus and continue your efforts, your organization will be pushed into the final stage of readiness.

STAGE 4: UNCONSCIOUS COMPETENCE

At this stage, you've been diligent in your efforts to vision, plan, and prepare. Operating at this level means that the plan is executed smoothly, professionally, and efficiently. The staff is well trained, the plan has been thoroughly rehearsed and revised as needed, and everyone is comfortable with their roles. People have practiced together. They know each other and the resources they will need, and they're ready to carry out the response to an extraordinary event as detailed in the plan. Although it will still produce stress, the extraordinary event won't create the uncertainty, discomfort, and disarray that it may have before this stage of readiness was reached. When your organization is truly ready, your customers and the community are protected to the best of your ability.

— *Security Planning in an Unstable World: A Public Official's Guide*
An abridged excerpt from Chapter 5

contaminants into the water. If an attempt was made to penetrate the facility, it would go unnoticed, because the facility had no detection equipment and no delay mechanisms. Significant amounts of graffiti inside the facility provided ample evidence that criminals were routinely breaching facility security without detection or intervention by water personnel or local law enforcement. City administrators were surprised by the vulnerability, because a city engineer and an employee of the public works department had conducted the vulnerability assessment.

Failure to implement appropriate countermeasures. In another instance, a large metropolitan community water system serving more than 100,000 customers had installed several electronic security systems. During the course of a revalidation of the recommendations from the original security vulnerability assessment, it was discovered that none of the installed alarms were being monitored. Management was surprised to learn that a breach of security at one of the facilities would have gone undetected until employees returned to work in the targeted facility. Again, no independent security professional had guided the risk assessment process. The utility had relied on the guidance of a security systems vendor, whose primary mission was to sell more products.

INVEST IN A SECURITY PROGRAM

Today, five years after 9/11, security has moved to the back burner at many facilities. But an incident can happen at any time, and community water systems must reinvest energy into their security programs. Numerous agencies continue to publish guidance that establishes industry standards on a balanced security program that safeguards drinking water and ensures adequate water for fire protection. In June 2005, the National Drinking Water Advisory Council published a report entitled "Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on Water Security Practices, Incentives, and Measures" (www.epa.gov/ogwdw/ndwac/pdfs/wswg/wswg_report_final_july2005.pdf). Utilities are advised to conduct an immediate gap analysis using the benchmarks in this guidance. The gap analysis results can form the foundation for a long-term security plan for each community water system. The report sets forth 14 recommendations:

Keypads limit access to restricted areas.

- Make an explicit and visible commitment of the senior leadership to security.
- Promote security awareness throughout the organization.
- Assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.
- Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.
- Identify managers and employees who are responsible for security and establish security expectations for all staff.
- Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.
- Employ contamination-detection protocols that are consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.
- Define security-sensitive information, establish physical and procedural controls to restrict access to security-sensitive information as appropriate, detect unauthorized access, and ensure information and communications systems will function during emergency response and recovery.
- Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower risk design and technology options.
- Monitor available threat-level information; escalate security procedures in response to relevant threats.
- Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans as necessary to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.
- Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, and customers.
- Forge reliable and collaborative partnerships with communities, managers of critical interdependent infrastructure, and response organizations.
- Develop utility-specific measures of security activities and achievements, and self assess against these measures to understand and document program progress.

Because an adequate VA makes up the foundation for any effective security program, a reassessment of the adequacy of the initial effort is critical for every community water system that is serious about safeguarding water. A security professional who is a Certified Protection Professional (CPP), Physical Security Professional (PSP), or Certified Security Consultant (CSC) with Risk Assessment Methodology–Water (RAM-W) experience should be involved in the process. Security is not an endpoint but a goal that can be achieved only through continued efforts to assess and upgrade your system. Water systems should review their vulnerability assessments periodically to account for changing threats or system additions to ensure that security objectives are being met.

Take a hard look at the effort extended in completing your risk assessment to decide whether an effective job was done by the right people or whether the process was simply an exercise to put another check in a regulatory box. The lives of community members, fire protection capability, and consumer confidence hang in the balance.

FOR MORE INFORMATION

- *Security Practices Primer for Water Utilities*, AwwaRF report
- *Distribution System Security Primer for Water Utilities*, AwwaRF report
- *Infrastructure Security Planning in an Unstable World: A Public Officials' Guide*
- *Safety First: Water Utility Security*, DVD
- *Security Practices Primer for Water Utilities*, AwwaRF report
- *Water Supply Systems Security*
- *Water System Security Field Guide*, book and video set
- *Water System Security: Biological Threat and Mitigation*, video