SHANNON SPENCE, COLUMN COORDINATOR
MARIE SHADDEN

Shadden

Developing a Security Culture

Physical security such as fences, access control, and closed-circuit television are critical to the protection of assets, organizational resiliency, and public safety; and utility managers have made great progress in enhancing physical security at their facilities. However, in the past few years the idea of creating not just secure utilities but resilient utilities has become a key focus of the water sector.

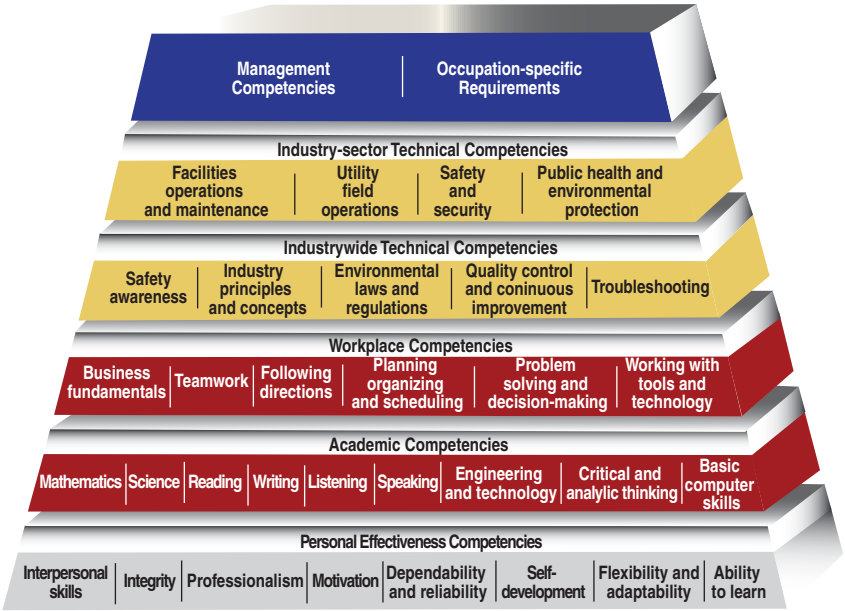
Significant progress toward utility resiliency has been made through improved emergency response capabilities such as those offered through the Water/Wastewater Agency Response (WARN) Networks. These WARN networks now in place all over the United States have bonded utilities together across large regions for the purpose of mutual aid.

The water industry is also beginning to embrace the idea of building a culture of security within the industry, and to recognize the vital link between a robust security culture and securing the delivery of clean water. Despite utilities' significant investments of time and money in vulnerability assessments, emergency response planning and training, the purchase and installation of expensive security equipment, hiring security guards, and development of security training programs, there still seems to be doubt about whether the development of an internal security culture is worthwhile.

What do we mean when we speak of a security culture? Building security into the day-to-day processes of utilities, such as including background checks when hiring employees, is one way of building a security culture. AWWA Standard G430: *Security Practices for Operation and Management* (2009) offers guidance on the use of background checks for employees, contractors, and temporary workers. It also recommends including security considerations in protocols for employee terminations, resignations, and other changes in status that would affect access. Although these are essential elements, alone they are not enough to grow a thorough security culture. The National Drinking Water Advisory Council (NDWAC) Recommendations on Water Security, along with associated performance metrics in the report the council issued in early 2006, address security in the organizational culture (USEPA, 2006). The metrics specifically focus on building a security culture, comprising one of the four component blocks of the NDWAC recommendations for effective water security. These include

- integration of security as intrinsic to the routine business and operations environment in the water utility,
- recognition of the importance of standard operating procedures,
- the explicit and visible commitment of senior leadership, and
- general promotion of security awareness.

FIGURE 1 Water sector competency model



BENEFITS

Although it is clearly understood that building and nurturing a strong security culture enhance preparedness, a security culture also has a number of benefits in terms of improving the efficiency of operations and the quality of the working environment.

Reducing loss. Where a security culture exists, managers seek to reduce the risk of loss caused by inventory shrinkage, frequent replacement of equipment, damage to vehicles, forgotten tools, abused or misused property, misappropriated assets and supplies, construction cost overruns, unnecessary overtime expenses, or mismanagement of worker's compensation or employee benefit funds. Such losses do not have to be "the cost of doing business."

Eliminating violence and intimidation. A strong, internal security culture protects both utility assets and employees. Employees will require less training and supervision in order to understand and meet security standards if these efforts become commonplace. In addition, employees tend to prevent the onset of workplace violence issues by reporting aberrant and bullying behavior. In a security-conscious environment substance abuse is often less tolerated because employees perceive it as being unsafe behavior around hazardous equipment and chemicals.

Customer concerns. A security culture within the organization can inspire greater public trust. Customers appreciate that utility employees are consistently accountable for high performance standards, safe practices, ethical behavior, and respect. Customer appreciation can show up in many ways—from volunteering to assist with "water watcher" programs to more patience with the utility during emergencies.

Enhanced readiness. Employees who have a heightened general awareness are more apt to recognize an aberrant event during routine operations and to exercise more initiative in bringing it to the organization's attention. Employees are also more likely to take personal responsibility for skills mastery, internal knowledge transfer, and safety, which all contribute to having a sustainable utility, and these employees are also more likely to perceive value in their organization and thus actively seek promotions to leadership positions.

WATER SECTOR COMPETENCY MODEL

For many other elements of a utility's comprehensive security program such as the design, procurement, installation, and use of physical security hardware; the funding of physical security improvements; and cyber security improvements, robust guidance is available. However, little guidance has been provided for water utility operators about how to internalize security into the culture of a water utility organization. In 2009 AWWA, the Water Environment Federation (WEF), and the US Environmental Protection Agency (USEPA)

collaborated on the development of the Water Sector Competency Model (USDOL, 2010), which defined the necessary knowledge, skills, and abilities for prospective water professionals.

The resulting model depicts core competencies that are desirable for field staff and operators, and it includes security elements. Most often this model is used as a tool for workforce developers, educators, and recruiters. However, the model can also be useful for managers and supervisors. AWWA and WEF have committed to promoting the use of the model and to keeping it current. The online version is interactive and provides a useful "checklist" that can assist in creating a "security culture."

As with most tools, scalability should be considered, and adoption of the recommendations will vary from one utility to another. Examples of the security culture competencies in the model include:

Analytic: identifies threats and risks, has external awareness, assesses information, and predicts outcomes;

Results driven: accountable customer service is a priority, problem solver, decisive, manages conflict, builds consensus;

Flexible, resilient: leads change, builds consensus and teams, partnering and followership come naturally, persuasive, leverages diversity;

Technically competent: seeks training, acquires new skills, effectively minimizes or mitigates losses, responds to crises, thrives on challenge.

Culturing a security environment can be assisted by staffing the utility through the recruitment, hiring, and promotion of employees who are already sensitive to and aware of security issues. However, it can also be nurtured through indoctrination, training, recognition, and reward. A security culture is one that explicitly demonstrates a preference for certain behaviors from the bottom up and then nurtures these same behaviors from the top down.

Tactics for recruiting security-conscious staff can vary. However, military populations are an excellent source for recruiting because they are already indoctrinated with a security culture and may also be trained with the latest technologies. In the current economy, prospects with recent US security clearances might even be easier to recruit because of diminished government budgets.

Situation-based questions in hiring and promotion interviews can reveal the values and behavioral inclination of the candidate. A scenario question is one in which the candidate is asked to describe what his or her action or response would be given a specific situation (i.e., avoiding yes/no answers); the question enables insight into the prospect's ability to analyze data and strive for results, and also explores what his or her orientation, motivation, commitment, and instincts to protect life and property are. Responses to scenario questions can be helpful in selecting hires and promotions that build a security culture. For example, will the prospect speak up if needed? Will the prospect follow established rules or seek improvements in security? Does the candidate have security awareness derived from broad experience?

BACKGROUND CHECKS

Many operators and managers question requiring a background check before hiring or promoting, and there is sometimes the sense that such an inquiry represents an invasion of privacy or that it might make hiring difficult because it may uncover the smallest infraction that will then need to be addressed. If in any doubt, always consult a human resources representative at your organization. In actuality a good background check should be considered critical before staffing a position that involves fiscal or public trust responsibility or significant customer interaction such as unsupervised visits to customers' homes. Many records are public and thus can be easily screened. However, the individual must give access to other types of personal information.

Probationary periods can also provide critical flexibility to a utility by allowing the hiring or promoting official or committee to ask clarifying questions. Disqualification during probation because of an unsuitability that surfaces during this time can save the utility money and reduce the risk of losses such as property and public confidence.

Building a security culture is a key part of having a resilient utility and is the result of continuous and coordinated effort throughout the organization. Furthermore, it can be built into the core competencies for all employees and will only strengthen the foundation for all other elements in a well-rounded security program.

— Marie Shadden is an independent public safety consultant in the Knoxville, Tenn., area where she assists government and private enterprise clients with response, security programs, and continuity plans and develops training for performance improvement in security, preparedness, and continuity. Her previous experience includes director of security and safety for the city of Atlanta Department of Watershed Management, a chief security officer, and a US Air Force Security Forces commander. Shadden received her bachelor's degree in criminology from the University of California at Berkeley and her master's degree in Public Administration from Golden Gate University in California. She may be contacted at mshaddenpub@gmail.com.

REFERENCES

AWWA, 2009. G430-09. *Security Practices for Operation and Management.* AWWA, Denver.

USDOL (US Department of Labor), 2010. Water Sector Competency Model. http://careeronestop.org/CompetencyModel/pyramid.aspx?WS=Y (accessed May 15, 2012).

USEPA (US Environmental Protection Agency), 2006. Active and Effective Water Security Programs, National Drinking Water Advisory Council Recommendations on Water Security. EPA 817-K-06-001. Ofce. of Water, Washington.

http://dx.doi.org/10.5942/jawwa.2012.104.0097