is also an issue that many utilities must deal with as they implement technology in their operations.

i. Physical Security

A good security system at a water utility will detect a threat, delay an adversary for as long as possible and aid in the response to the threat. These requirements are really no different than those for any other critical infrastructure. Physical security systems are the nuts and bolts that do the majority of detection and delay.

Deterrence should be the first line of defense in security. Area lighting, fences and barricades are simple, passive measures that are put in place to deter malevolent acts and trespassing. Vehicle barriers near critical facilities such as chemical storage buildings prevent an explosive device delivered by a vehicle or use of the vehicle itself as a weapon. Barriers also serve the purpose to prevent accidents with vehicles and heavy equipment around buildings and tanks.

Cameras and motion sensors are examples of more sophisticated, active security measures. An important point to make is that high-tech security tools such as cameras and motion sensors are only effective if they have someone monitoring them. Once monitoring is in place, the threat must be assessed and identified as such in order for effective detection to occur at all. Cameras may also act as a passive deterrent if they are positioned in clearly visible

locations. This prevents an adversary from thinking an act can be committed unobserved.

ii. Cyber Security

The need to protect a water utility via its computer system is often underestimated. Communications networks and supervisory control and data acquisition (SCADA) can be used against a water system and can easily compromise an operation. A SCADA system should be completely isolated from all other network connections, especially those connected to the internet. A water system's connection to the internet provides an access point for external parties to potentially control and disrupt a system. A computer firewall is an example of an effective way to block cyber hackers. Intrusion-detection software is available that alerts malicious network activity from external and internal sources. Factory default configuration settings are often not adequate to protect an entire system. Passwords should be regularly changed and a data log should be installed that can track all activity on a SCADA system. Few personnel should need full access to SCADA control and it should not be accessible on all computers.

Water treatment facilities have unique requirements in terms of limiting access. There are many different types of areas such as chemical feed areas, office space, computer rooms and storage areas. Gates, doors and padlocks often are what protect access to these areas. Managing access can be a difficult task with many sets of keys. The Atlanta-Fulton Water Commission

(AFWC) has simplified the tedious task of traditional key and lock management. An electronic locking system enables a single key to open only the locks that are appropriate for specific personnel's access rights. This system allows the system operators to block access for lost or stolen keys, obtain a complete audit trail from a key or lock and control access to all locks at the facility by programming access to them through a software program (Journal AWWA, May 2004).

b. The Soft, Chewy Center

It is not expected that a chain link fence will prevent an intruder from gaining access to a facility. An alarm sounding from an opened hatch on a water tank will not stop an adversary from contaminating a water supply. It is the "insides" of a system that do the real detection and response in security management. These are the people who are trained to follow guidelines and procedures. These are what protects the integrity of the water system once a threat is past the first layer of protection.

i. Policies and Procedures

Policies and procedures for everyday security management and for emergency are the heart and soul of security management. Well-written policies and procedures are only effective with proper implementation and continual training of employees. Policies and procedures are worth only the paper on which they are written, if they are not adhered to and enforced. The

challenges are in writing these guidelines so they are meaningful to a specific utility and receiving honest support from personnel.

Most water utilities have policy manuals that outline and define rules for working on site and relationships on a utility and personnel basis. These manuals should be accessible and be kept updated regularly. Policies related to how a system operates and why certain functions happen can be important to adding security or changing the way things are done in some way. Procedural guidelines relate more to responsibilities and who does what and when. Security procedures at a water plant are important in maintaining a secure site and safe operation, and especially important in emergency situations. Emergency procedures should be practiced on a regular basis and updated as new equipment and chemicals are added.

Equipment and chemical deliveries to a water treatment plant occur daily. It should be required that companies schedule all deliveries in advance, notify the plant with picture identification of delivery personnel and follow check-in procedures with all deliveries. Similar check-in procedures should apply to visitors and contractors working on site at the plant and facilities.

Performing background checks of potential and current employees is becoming a more common practice in the water utility industry. Background checks should be done prior to hiring an employee and upon any major change in position or access rights for a current employee. Background checks should also be requested by the utility for chemical delivery personnel.

Water utility vehicles can easily be targets of vandalism or used as weapons. A key audit for all vehicles and facilities should be done regularly. This involves accounting for all keys, documenting number of keys and which personnel have access to which keys. A consistent key audit will let a utility know if keys are disappearing and what level of access employees have to facilities, and in turn, how secure those facilities are.

Operationally, security measures can include everything from informing law enforcement about a current threat to using surveillance systems and dedicated security personnel to keep watch on a certain facility. Sometimes even the simplest security measures such as locking doors and putting away loose tools are not practiced. These are examples of no-cost solutions that are easy to identify, but often difficult to train personnel to get into the habit of doing.

Vehicle inspections have been used increasingly at water treatment plants. An under-vehicle inspection ramp employs a heavy-duty speed bump ramp. The ramp allows the underside of the vehicle to be examined for any type of hidden device by video. The video signal is sent to monitors inside an office, allowing vehicles to be inspected in a safe and fast manner (Journal AWWA, February 2002).

ii. Managing People

People are really what make a security system effective, or ineffective. When security management is examined, managing people is what the success of all

the high-tech physical components and brilliant policies hinges on. As mentioned previously, training is a crucial component of overall management. In the case of water utilities, you are often training technicians and professionals in the field of water treatment to be more security-minded. This is not inherent and nothing should be assumed.

During a crisis, water utility personnel will have concerns of their own and their family's personal safety. This could affect decisions and performance. This is why continued training, education and reinforcement of emergency response procedures is essential.

A common mistake is a water utility believing that "it can't happen here" and ignoring security concerns. This attitude stems from the misunderstanding of a system's vulnerabilities and a misconception of threat level. For example, a small, rural water system is not likely a target for a complex, organized terrorist attack. That, however, should not be the level of threat considered for such a system. It would not be practical nor possible to protect against such an attack.

Maintenance is another key component of managing a security system. Aging equipment within a water system is a common problem. Old and under-maintained equipment is a vulnerability in a couple of ways. If a piece of equipment breaks down, it loses its function and is a liability to the system. A poorly operating pump or valve is also much easier for an adversary to

overcome. Regular condition checks of fencing, lights, alarms and cameras are also necessary to maintaining a security system.

Managing people to be aware and trained to secure a water system also involves a component of the public. The public should definitely know that their water supply is secure and safe. They should also be educated to be aware of what is happening at water facilities in their neighborhoods and to report suspicious activities. However, the over-cooperative plant operator can easily give too much information. Since security at water systems has received increased attention recently, some operators are anxious to show the public all the wonderful improvements to the plant and all the fancy security features. The innocent showcasing of a facility's security system may be unnecessarily indicating the most vulnerable locations to the public. Another common practice that is changing is posting system information posted on a municipal website.

iii. System Operations

Today, water system operators face more than just the task of operating and maintaining a safe water supply. Part of their mission now includes integrating and managing security systems and implementing security emergency policies and procedures that may not have been in place before.

Security should not negatively impact how a water plant and system operate. Ideally, security systems should complement operations. This can be done a

number of ways, but it takes coordinated planning involving designers and operators.

Devices such as early warning monitors for water quality can be used to monitor chemical residuals and detect contamination. Consumers expect that immediate sampling and testing would occur in response to a threat or suspicion of system tampering (States, 2003). These expectations also have required that some additional monitoring be conducted on a regular basis and more frequently during heightened national alert.

A common weakness among many utilities is the lack of operator knowledge in regards of how to manually operate the system. So much of today's water system operation has gone to automation that the basic knowledge of when and why certain valves and filters are operated is lost. Particularly in emergency situations this is a critical function.

iv. Funding

It must be understood that every scenario cannot be protected against. No matter how much money is spent on fences, alarms and training, a determined adversary will accomplish their goal. Funding and resources are limited and stretched at nearly all water supply facilities. Therefore, risks must be weighed against available resources in the analysis of the potential threat. The higher the threat level and more sophisticated the adversary, the more resources required for protection. There is currently no available federal or

state funding to assist water systems with the implementation of security systems. This may not always be the case, but in the meantime, utilities must be performing cost-to-benefit analyses when spending money on security. The difficult task is determining benefit when assessing potential threat levels and quantifying consequences.

v. Public Relations

Public perception is a factor that must be considered when dealing with protecting water supplies. How safe the public perceives their water supply to be can be nearly as important as its actual safety. This is best handled through public education and good communication. What water systems must strive for in a community is a "neighborhood watch mentality". Water systems, by the nature of their function, have facilities integrated in residential neighborhoods. Pump station buildings, fire hydrants, storage reservoirs and water meters are literally next door to residents and can provide direct, open access to a water supply. Through public education, citizens can be taught where and what water facilities are and to contact police if they see any suspicious activity. This distribution of information must be done in a manner that does not disclose too much information that a system may be compromised.

Water utilities should pay particular attention to customer complaints involving illnesses. Most chemical and biological contaminants cause disease symptoms. Loss of water pressure is a complaint that may signal an attempt

to overcome the pressure in a water system. Complaints involving access such as unattended running fire hydrants and nonutility personnel on private property are also of particular concern. Public awareness is often a utility's best defense in risk management (AWWA, November 2004).

vi. Safety

Security is often mentioned in the same breath as safety. These are terms used synonymously in many cases and although they have different definitions, they are not mutually exclusive. Many security applications can also be considered safety measures. For example, protecting chlorine gas cylinders in locked, contained rooms and using jersey barriers serves multiple purposes. Containing the gas cylinders minimizes the risk and consequences of an accidental release. The same buildings and barriers that keep a chlorine leak contained, keep intruders away. Jersey barriers help prevent a vehicle or piece of equipment from intentionally, or accidentally damaging the chemical feed room.

Security functions at a water plant in the same way that safety does. Both are only truly effective if personnel are trained to follow guidelines and procedures. It should be analyzed whether systems installed for safety can be used as security, and vice versa. Handrails and covers around and over open water tanks are an example of features that serve both in a safety and security function. Sensor alarms that indicate higher than normal levels of chemical are another instance where normal operating features serve a security role.

c. Proposed Strategies

The following are proposed strategies that will likely benefit water systems when considering security management. These are suggestions that often combine management of risk and management of operations at infrastructure facilities.

i. Early Detection

Among larger water utilities, there needs to be an increased focus on early detection. No system can prevent everything, but early detection and early response can reduce risk significantly. For example, it would be nearly impossible to sufficiently protect the number of fire hydrants that most communities have in service. Preventing an adversary with a tanker truck from hooking to a hydrant and overcoming system pressure with some chemical would be difficult. However, the earlier the contamination can be detected once it is in the system, the faster a response can happen and recude consequences. Early detection devices for water contaminants are becoming more widely available, affordable and expected by the public. Devices that deliver real-time information to the system operator should be installed at locations where there may be opportunity for introduction into the system and widespread contamination.

ii. Prioritization

Sometimes, the most obvious, accessible way to compromise a water system is that which can cause the most damage. The most accessible facilities, or

"low-hanging fruit", will be the first to be attacked are often easy to correct and should be given priority.

Approximately 15% of the water and wastewater utilities in the U.S. provide service to more than 75% of the population (Copeland, 2002). It seems that the utilities serving the majority of the population would be at the greatest risk and deserve the most protection. The smaller systems in more rural areas are often far less protected and less prepared for an attack. A successful attack on these smaller systems would likely cause local panic, economic impacts and a loss of public confidence in water supplies. However, it is the large systems that serve metropolitan areas that are spending millions on security and preparation for an attack.

iii. Redundancies

Having an inventory of critical equipment is a necessity, if a utility is financially capable of doing so. If a critical valve were damaged or a pump were to fail, back-up equipment can be on-hand for replacement. It is important that stored equipment should be kept in a separate location from the operating equipment. If the operating equipment were damaged by an attack, the spare equipment should not be risked as well.

Creating redundancies within the system allows for multiple paths when one part of the system is compromised. A coordinated attack on a system can take

out several areas of a system. Redundancies improve the chances of a utility being able to recover quickly.

iv. Increased Cooperation

The idea of securing public water systems against potential threats can imply to some an isolation or "walling off" from the rest of the world. This can be a threat in and of itself. Water systems need to be in the practice of sharing information to the extent possible. This involves smaller systems working together to learn important lessons about their vulnerabilities through open discussions. Many small systems have a history of cooperation and sharing operational information between one another. In order for the same to happen with regards to security, there must be trust between the two utilities.

Not enough relationships exist between other municipal, local officials and public water utilities. Fire departments, departments of health, law enforcement agencies, energy utilities and local emergency services should all be working in conjunction toward a common goal of protecting the water system and responding to threats and incidents.

d. Long Term Effects

There will likely be several long term impacts on the water and engineering industry as a result of this new emphasis on security. First, it will change the way we look at water systems and infrastructure in general. Not only are they what make up quality of life and communities, but they have become potential targets for

people who are trying to do us harm. Secondly, security will be incorporated as a design consideration for water and other infrastructure. This may involve additional redundancies, more cameras and alarms or barriers and blast-proof structures.

Another long term effect is that the trend in monitoring water systems will increasingly be focused on the ability to detect problems in real-time. The ability to respond to a situation quickly and correctly can save lives and minimize damage. New and improved technology will allow such systems to be more commonplace and affordable. New devices are already emerging that use robotics to take water samples and report real-time data. Computer-controlled sensors float on water sources, collect data on water temperature, oxygen, salt content, phosphorus, ammonia and other substances that are key indicators of certain chemicals that may be polluting the water. This data is transmitted via cellular phone signals to a main computer. It can then be determined, nearly instantaneously, if the water is suitable for consumption. Researchers and companies are working on more affordable, disposable sensors (CNN.com, May 2004).

Security-conscious engineering firms that recognize this new market and need in the industry will be successful in the long term. *The 2003-2006 Municipal Water & Wastewater Market for Design and Construction Firm* report, released in June of 2003 by a Massachusetts management consulting company, Zweig White, states that larger engineering design firms have begun to combine security considerations

with design work (Landers, 2003). Although highly competitive, the sector offers thousands of potential clients.

V. Summary and Conclusions

When identifying, implementing and managing security at water system facilities, there are many issues that must be considered. Initially, defining what risks exist for a system may be the most critical step to managing that risk. How to deal with that risk is a matter of considering existing structures, procedures and policies and what are the most practical solutions. Management of security operations requires not only knowledge of the security systems themselves, but a relationship with the public and an understanding of local laws and safety issues.

a. The Four P's

This paper has discussed a number of topics relating to risk and security management at public drinking water systems. These discussions can be summarized into four general topic headings. In assessment of threats to a water utility, the study should be **practical**. Realistic goals for threat assessment and risk abatement should be considered. **Prioritization** of critical assets at a facility and water use in emergency situations should be analyzed and applied when allocating resources. In many cases, security features at a water system are already in place in the form of safety. **Planning** in advance and as part of risk management can identify these features and eliminate unnecessary costs. **Public involvement** in security is crucial not only because the public is a resource to monitor critical infrastructure in the community, but because as the customer, they have a right to feel their drinking water is secure.

b. Suggestions for Additional Work

A vulnerability assessment is essentially an analysis of strengths, weaknesses, opportunities and threats (SWOT). Infrastructure as a whole, and water systems in particular, will likely periodically update their assessments with a version of a SWOT analysis. A subject that would be of interest to follow in the coming years is how closely infrastructure mimics examples of SWOT analyses in the business environment.

Roughly two out of every three large municipal water systems in the United States have already or intend to contract with design or construction firms for security-related projects (Shuster, 2003). Design firms hoping to make security a business opportunity, will face tight competition. Security is here to stay and design engineers can expect to incorporate increased security into new construction and rehabilitations. An analysis of this market should be done to determine available opportunities for studies and security design services.

There are currently no federal or state requirements for specific wastewater security. However, HR 866 "Wastewater Treatment Works Security Act of 2003" has been approved by the House Transportation and Infrastructure Committee in February 2003. This bill would make available to public wastewater treatment facilities $220 million for security studies and physical improvements. There is potentially an entirely new market of wastewater security in the near future.

REFERENCES

American Water Works Association, "AWWA News Release", http://www.awwa.org/advocacy/pressroom/pr/020612.cfm, (cited August 12, 2004).

American Water Works Association, "We Need Our Customers to Complain", *Opflow*, Vol.30, No. 11, November 2004.

CNN.com, "Robots May Protect Drinking Water from Terror Attacks", http://www.cnn.com/2004TECH/05/04/water.robots.ap/index.html, (cited May 14, 2004).

Copeland, Claudia and Betsy Cody, Terrorism and Security issues Facing the Water Infrastructure Sector", Congressional Research Service, February 2002.

Ginley, Dennis. "Technology Solutions for Physical Plant Security", *Journal AWWA*, February 2002, p. 46.

Journal AWWA, "Protecting Our Water – Drinking Water Security in America After 9/11", July 2003.

Journal AWWA, "Tightening Access Within Water Treatment Facilities", May 2004, p. 44.

Landers, Jay, "Security Needs Offer Opportunities, Study Says", *Civil Engineering*, August 2003, p. 29.

Locy, Toni. "Court Strikes Down Patriot Act Provision", USA Today, September 30, 2004, p. A.3.

Lowery, Philip S. and Jennifer N. Handy, "Dam Security in a New Era", *CE News*, June 2003, p. 28.

Shuster, Lauri A., "Bridge and Tunnel Security", *Civil Engineering*, Vol. 74, No. 9, September 2004, pp. 41-49.

States, Stanley and Michele Scheuring, "Utility-based Analytical Methods to Ensure Public Water Supply Security", *Journal AWWA*, April 2003, pp. 103-115.

GLOSSARY OF ACRONYMS

AFWC	Atlanta-Fulton Water Commission
AWWA	American Water Works Association
AWWARF	American Water Works Association Research Foundation
EPA	Environmental Protection Agency
ERP	Emergency Response Plans
PCCIP	President's Commission on Critical Infrastructure
RAM-W	Risk Assessment Methodology for Water
SCADA	Supervisory Control And Data Acquisition
SWOT	Strengths, Weaknesses, Opportunities and Threats