



Water Utility Security: Challenges and Solutions

By James T. McGowan



1105 N.E. Circle Blvd., Corvallis, OR 97330
541-738-5500 • Fax 541-738-5501 • www.cyberlock.com • sales@videx.com

Water Utility Security: Challenges and Solutions

The repercussions from 9/11 and continued terrorist threats have put increased pressure on water utilities to secure their physical assets and electronically track anyone that accesses their facilities. Acting under the authority of Congress, the Environmental Protection Agency (EPA) has developed vulnerability assessment guidelines to help water utilities evaluate their susceptibility to potential threats and identify corrective actions needed to reduce risks. Although the EPA is our country's designated water utility enforcement agency, there are no provisions in the water security regulations that give the EPA authority to enforce compliance. Nevertheless, a growing number of water facilities consider security essential to their operations and are giving it precedence.

Taking the Practical Approach to Security

Water utilities, both large and small, are looking for solutions that will allow them to secure their perimeters, track the movements of individuals, and prevent unauthorized access to their physical assets. In doing so, they face some unique challenges. Entry gates, well sites, re-pumping stations, chemical feed and other sensitive areas need to be protected. Scheduled water sampling should be electronically documented. Last but not least, utilities are tasked with managing the access of their subcontractors and vendors. Taking a practical, measured approach to sourcing security solutions makes the task more productive and less intimidating.

Will Security Impede Daily Operations?

Water utilities must be progressive in looking at what they perceive to be a security need because security can be considered intrusive not only by staff but by those that are maintaining the system. The challenge is to raise overall security without it becoming a barrier. A utility must have clearly defined goals that will support, not impede, daily operations. There are some things to consider when evaluating a potential access control solution:

- How must employee work processes change in order to accommodate the system?
- What are the recurring costs of maintaining the system? How much time and in-house resources are required for managing the system? What will be the administrative costs to support the system?
- What wiring and structural changes would be required for installing the system? How will asbestos containment issues be avoided?
- How will the system electronically secure sensitive areas that have no available power?
- Is there flexibility to expand the system on a limited budget? Can the system be easily integrated with other access control solutions?
- Are sufficient funds available to fund the system?

When targeting a "solution" for security, it is easy to get tunnel vision. It is important to keep the big picture in mind and think about how each solution will affect daily operations. The goal is to improve security, not create more problems. In summary, ask: Can we do it? Do we have the people to do it? How many man-hours will it take? Do we have to change the way people currently do things? Will it negatively affect any of our processes?

Gaining Acceptance

No matter how beneficial the security solution might be, if management does not accept the system, it will not be successful. Here are suggestions for gaining acceptance:

- Involve the managers early on as acceptance from the top will flow down throughout the organization. Managers can help pinpoint specific areas and security concerns. Make them a part of the process and the proposed solution will quickly gain their support.
- Identify departments and processes that will be positively affected by adding security and share this with the managers. After reaching a general consensus, roll out a plan-of-action that includes immediate and long-term security goals.

Keeping It Simple

Utilities need manageable security solutions that allow them to track multiple identities and control access to physical assets spread out over large geographic areas. The task of researching choices may be daunting but well worth the effort. The simplest approach is to:

1. Prioritize identified security weaknesses.
2. Determine those that most urgently need to be addressed.
3. Integrate practical solutions that support day-to-day operations while minimizing risks of sabotage and theft.

Getting Acquainted with Today's Technology

Once a utility has obtained general consensus of their security needs and established immediate and long-term goals, they can roll out their plan-of-action. It's best to have some knowledge of the different types of systems in today's market so the right questions can be asked as they pertain to a specific utility's requirements.

Multi-location Digital Video for Outdoor Surveillance

Multi-location digital video security systems are a viable option for those that want to set up an efficient outdoor surveillance system. When evaluating video solutions, be aware that the equipment has to stand up to tampering, extreme weather conditions, and varying levels of light. As the technology has evolved, visual-light cameras are more compact and are able to produce images under a wider spectrum of light conditions. Thermal imaging cameras in conjunction with analytics and sensors can be used in areas that have no lighting. Live cameras along with an integrated alarm system can be beneficial to utilities that have a security command center that operates 24/7. It can be quickly determined whether an intrusion is non-threatening or something more serious.

Will the Video Files Be Too Big to Handle?

When considering video, note that video files are extremely large and can present challenges to network bandwidth. Bandwidth and file size are closely related to each other. The larger the video image, the larger the bandwidth one needs to transmit the image over a network. When a large number of cameras are installed over a widespread area, compromises usually have to be made in regards to the level of image quality and the number of images reproduced each second. Essentially, digital signals of the images need to be processed and transmitted over the network in a reasonable length of time.

Wireless Video Verification for Securing Areas without Power

Wireless video verification can be considered for utilities that have areas to secure but no available power from which to draw. These systems combine battery-powered cameras, sensors, and GPRS radio communication with a central monitoring station. Video verified intrusion alarms are becoming popular as the costs of CCTV have been declining, making it a practical solution for locally enhanced security.

Are Security Cameras Enough?

For water utilities that do not have personnel monitoring their security 24/7, cameras may not be enough. While cameras may act as a deterrent, they are only one piece of a comprehensive access control solution. Cameras are for observation, not prevention. Cameras cannot control individual access to a facility's physical assets. In most situations, they will not protect a utility from vandalism and theft. Most of all, a video camera system cannot provide the key control and electronic audit reporting water utilities need. The good news is there are key-centric and lock-centric access control solutions available that complement the capabilities of a video camera system.

Key-Centric Solutions

With a key-centric system, the concept of a smart lock is reversed. Key-centric systems interface with software primarily through a smart key that powers the lock. Instead of the processing taking place within the lock, the intelligence is in the key. A key-centric system usually includes smart padlocks, programmable keys, and electromechanical lock cylinders. Easy to install, the system uses the lock hardware already at a facility. As no wiring or power is required for installation, a utility's existing mechanical locks can be quickly converted to electronic locks simply by replacing each mechanical lock's cylinder with an electronic cylinder.

One such key-centric solution is the CyberLock system by Videx that offers over 280 electromechanical cylinder designs for installing in lock hardware on everything from doors to cabinets to underground water sample stations . . . nearly anywhere a mechanical lock is present at water utility sites.

Key-centric access solutions are virtually tailor-made for water utilities. A utility can have electronic access control and auditing throughout their facilities regardless of whether or not power is available to the site. They can control who and when someone can open a gate, enter an office, or access sensitive areas. The audit reporting capabilities of this type of system can be valuable when the EPA requests electronic documentation of traffic in an area where there have been security issues.

Lock-Centric Solutions

A lock-centric access solution where the power resides in the lock itself is well-known technology that is commonly seen at the door. There are many on the market from which to choose including smart card, digital keypad, key fob, video entry, biometric door access systems, and more. Some require wiring at installation and operate on local power and others are battery-operated. The typical lock-centric solution cannot be expanded to entry gates and areas where wiring is not feasible. Most have full access control capabilities including audit reporting and restricted access.

It's best to assess each product's features and drawbacks before deciding which system best suits your operations. Take note that lock-centric door entry technology will soon offer smart phone integration capabilities.

Biometrics and Dirty Fingers

Biometrics at the door once fascinated "Star Wars" and "James Bond" movie fans. Today, biometrics is considered mainstream and many of the features of biometrics are scaled-down technology from military systems. Although single door systems that use biometrics are becoming more affordable, large biometric applications can still be impractical because of the cost of replacement hardware and installation. Also, a large amount of memory is required to store biometric templates. Unlike what we see in espionage movies, misreads caused by something as simple as a dirty finger can fool many systems. Keep an eye on this technology as it is evolving rapidly.

Perimeter Protection Solutions

To protect a water utility's perimeters, there are physical security solutions that typically include fence intrusion monitors, photo-beam towers, infrared illumination devices, and motion detection towers. Each can be helpful when installed at strategic locations utility-wide. It's important to pre-determine the manpower and equipment required to gain some or all of the benefits of this type of solution. For example, will the system automatically initiate a security response? Will someone have to be actively monitoring the equipment's receivers in order to know that an intrusion event is taking place?

Don't Drop the Ball

In closing, all of the products mentioned are certainly capable. However, implementing an access management solution is just the beginning. Utilities must not become complacent and think that "everything is now safe and secure because we have a security system in place." To succeed, they must follow up with education, on-going training, employee awareness, and enforcement.



James T. McGowan is VP of Sales & Marketing at Videx, a company that designs and manufactures CyberLock and Flex System access control solutions for utilities. For more information go to www.videx.com or call 541-738-5500.