CyberLock®

Innovative Solutions
Water Security

CyberLock®

Security Challenges in the Water Industry

Water utilities, both large and small, are looking for solutions that will allow them to secure their perimeters, track the movement 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. Additionally, scheduled water sampling should be electronically documented. Last but not least, utilities are tasked with managing the access of their subcontractors and vendors, which can be challenging to their security. Taking a practical, measured approach to sourcing security solutions makes the task more productive and less intimidating.

CyberLock is virtually tailor-made for water utilities. With CyberLock, a utility can have electronic access control and auditing capabilities throughout their facilities, regardless of whether or not power is available to the site.

SOUTH TAHOE PUBLIC UTILITY USE CASE

South Tahoe Public Utility District ("South Tahoe") is the largest water provider and the sole sewage treatment facility for South Tahoe, servicing 14,000 residential water connections, 660 commercial & government sites, and 17,000 sewers. South Tahoe uses SCADA (Supervisory Control and Data Acquisition) software, in conjunction with Wonderware InTouch® software, to automate their processes for moving water and sewage through South Lake Tahoe. While SCADA and Wonderware InTouch® were capable of automating processes throughout the district, South Tahoe realized they needed an access control solution at their remote sites. "We did not have SCADA out at remote facilities before - this was a new venture for us," states Chris Skelly, IT Manager for South Tahoe.

Challenge: Eliminating Passwords and Securing Remote Sites with SCADA

For South Tahoe, security, specifically safeguarding facility assets, is a top priority. Through SCADA, they implemented a policy requiring that all system passwords contain at least 15 characters. However, remembering complex passwords and expecting administrators to track multiple passwords across resources presented its own challenges. It soon became clear that South Tahoe needed to simplify its procedures, yet compromising on the security of its facilities was not an option. Rather than requiring its crew to remember a second 15-character password just for the remote sites, South Tahoe turned to the CyberLock system.

Passwords within SCADA protected South Tahoe's pumps and generators, including those at the Luther Pass Pump Station site. This facility exports all of the treated wastewater out of the Lake Tahoe Basin to the Harvey Place Reservoir, on their Diamond Valley Ranch property. The Luther Pass Pump Station regulates up to four million gallons of wastewater daily, all of which is controlled by the SCADA application. South Tahoe is held responsible for any effluent that touches the ground or escapes the system. Accordingly, securing the application that is ultimately responsible for controlling the flow of waste is of the utmost importance.

Solution: CyberLock

South Tahoe installed CyberLock to secure remote SCADA applications that controlled the operation of pumps and generators. Mission critical software is secured with CyberKey smart keys, rather than a password. CyberKey smart keys are programmed with scheduled access permissions, permitting access only during certain dates and times. South Tahoe personnel are given an access schedule within their assigned CyberKey. During their shift, the CyberKey will open the SCADA application, allowing the operator to start or stop pumps and generators. However, outside of their assigned shift time, the CyberKey smart key will deny access to the SCADA application, recording details of the unauthorized access attempt.

Now that access to critical facilities is protected by CyberLock, Chris Skelly explains "We no longer worry about the SCADA application going unattended," and adds that there is no longer cause for concern "if a disgruntled employee, or a member of the public comes in and tries to access the application."

Another added benefit is that the CyberLock system can be hosted entirely by South Tahoe, on its own servers. With sites located far from the major urban centers of Reno and Sacramento, South Tahoe does not always have access to a reliable Internet connection, meaning cloud and web-based platforms are not practical. With CyberLock, South Tahoe is even able to provide smart keys to other departments, such as natural gas, electric, and miscellaneous contractors. With CyberLock's comprehensive audit trail data, stored in both smart keys and locks, South Tahoe can monitor the whereabouts of each key.

Since adopting CyberLock over 10 years ago, the system has surpassed South Tahoe's needs and expectations. With hundreds of locks, padlocks, and keys currently deployed, South Tahoe has continued to expand their CyberLock hardware and software. Through SCADA and CyberLock, South Tahoe ensures that the public can continue to enjoy drinking, swimming, and recreating in the pristine, beautiful waters surrounding the Lake Tahoe Basin.

CyberLock Features

Remote Access Control

CyberKey smart keys provide all the power to the lock cylinder; therefore there is no need for hard-wiring, making CyberLock the ideal solution for remote locations.

Control and Schedule Access

Using the CyberAudit Management software, permissions for each lock and key can be changed effortlessly, enabling immediate and precise control over access to all entry points. CyberKey smart keys are programmed with a schedule to open one, several, or all locks in the system within a designated time frame.

Increase Accountability

Every time a CyberKey meets a CyberLock, a time-stamped access record is stored in both the lock and the key, providing system administrators with full visibility of all access attempts, whether successful or not.

Physical Security

Unlike mechanical locks, CyberLock cylinders have a unique, sealed design that negates standard lock picking techniques. CyberLock cylinders are designed to withstand a variety of harsh conditions while maintaining security. CyberLock padlocks are IP68 rated.

Key Control

When a key is lost or stolen, CyberLock cylinders can be programmed to deny access to the lost or stolen key. Additionally, CyberKey smart keys can be scheduled with an expiration date. This means when the key expires it will deny access until communication occurs between the key and the CyberAudit software.

Easy Installation

Over 380 CyberLock cylinders have been designed to retrofit into a variety of access points, including doors, padlocked gates, containers, equipment, safes and more. CyberLock cylinders retrofit directly into existing hardware, making installation quick and seamless.

How it Works: A Simple Step-by-Step Process

Step 1

Replace existing mechanical cylinders or padlocks with a programmed CyberLock cylinder. Each CyberLock is an electronic version of a standard mechanical lock cylinder. Installation is as simple as removing the original cylinder and replacing it with a CyberLock cylinder. Installation requires neither wiring nor batteries, making it quick and easy.

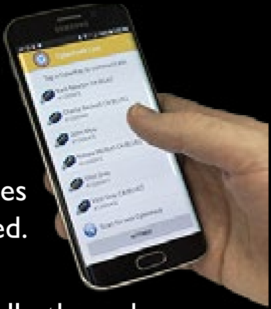
Step 2

Assign a CyberKey to a user. Keys are programmed with access privileges for each user. A standard key holds a list of locks the user may open, with a schedule of days and times when access is allowed. For instance, an employee's key can be programmed to only open their assigned locks Monday through Friday 7 A.M. to 5 P.M.

Step 3

Access locks. When a CyberKey meets a CyberLock, the cylinder is energized and an information exchange occurs to determine if the key has access to that specific cylinder. The event and time is stored in both the lock and key. Lock cylinders and keys also record when an unauthorized attempt to open a lock occurred.

Step 4



Download audit trails and update keys via communicator devices. Expiring keys regularly ensures users frequently update their keys. When validating keys, the system downloads the audit trail and uploads new access privileges to the key. An expired key will not work until it is updated.

Step 5

View audit trail. The CyberLock system is managed centrally through CyberAudit software. Customized audit reports and notifications on suspicious activities can be automatically generated via email.

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