The Role of Lock Systems in Protecting Critical Infrastructure

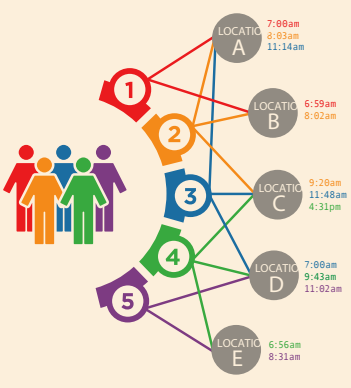
Security: Never optional. Now imperative.

Almost everywhere, the fabric of modern society rests on a set of technically dense systems commonly referred to as critical infrastructure. On the upside, this networked flow of water, goods, traffic, power, information, communications, fuel and finance delivers unprecedented benefits and a steady rise in quality of life. At the same time, it presents vulnerabilities heretofore unimagined. The failure of a single substation can bring down the power grid of an entire region. A breach in a lone data center can cause monetary chaos a continent away. An erroneous maintenance procedure can put multiple aircraft in serious jeopardy.

While technical flaws in such systems may be subtle and complex, they remain repairable through sound engineering practices. Unfortunately, human causes represent a very different case. History has repeatedly demonstrated that crime, vandalism, terrorism, and other socially aberrant behaviors are an enduring fact of life. And so it is that security measures have become a permanent fixture in modern organizations at nearly every scale, from global transport to local wastewater treatment.

Adequate security is a multi-dimensional challenge.

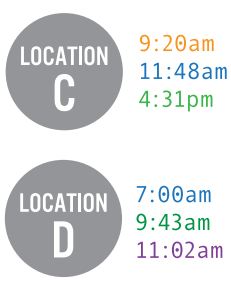
In times past, security management largely concerned itself with the physical aspects of asset protection. Locks, doors, cabinets, gates and other such barriers formed the basic core. However, the complexity of modern organizations has introduced a new set of challenges centered on the administration of access control: Who can get to what and when, and under what circumstances? Often, a broad and dynamic mix of employees, subcontractors and other parties must be accounted for when adhering to established security policies.



As a result, the interface between security assets and personnel becomes a very challenging part of the management task. To be effective, the system must provide adequate protection; yet avoid compromising an organization's efficiency and productivity. At the same time, it must be implemented in the most cost-effective manner possible.

Physical security must be reconciled with administrative security.

To this day, locking devices remain a mainstay of physical security. Often, they form the very foundation of an organization's bulwark against outside intrusion. That said, they are only as effective as the administrative systems that control their deployment and use. Frequently, you operate within a diversity of user populations, each requiring its own level of access. Subcontractors might be cleared for maintenance areas, but not laboratories, and so on. A running inventory may be required to track access devices and to keep a traceable record mandated by regulatory bodies.



Remote sites pose unique vulnerabilities that require specialized solutions.

Physical proximity plays an important role in an organization's security architecture. Central plants and administrative facilities provide ample opportunities for sophisticated systems that extend to electronic locks and video surveillance. Remote sites, on the other hand, do not. For the most part, these sites rely on conventional mechanical locks to secure critical access areas, such as cell towers, gates, well sites, server racks, traffic control cabinets, re-pumping stations and chemical feed stations, just to name a few.

These antiquated mechanical locking systems present numerous administrative challenges. Conventional keys are untraceable and easily duplicated. Often, management loses track of how many keys are currently in service and, perhaps more importantly, who they're assigned to. In many instances, keys may remain in circulation even after their owners no longer have access privileges, opening the possibility of malicious behavior. Consider the case of a subcontractor who is laid off but fails to turn in their key and can't be contacted. Nothing short of replacing all the locks will fully remedy the situation—a painful but sometimes necessary solution.

Also, locks themselves become a point of vulnerability, especially at remote sites. The keyway in mechanical locks leaves them vulnerable to being picked. This may render expensive or mission-critical equipment exposed to theft or vandalism.

In short, conventional lock and key systems often fall far short of providing an adequate level of security in many critical infrastructure industries.

At CyberLock all locks are not created equal—by design.

CyberLock offers a highly efficient and cost-effective method of implementing and maintaining an access control system, regardless of how or where the locks are dispersed. It centers on a combination of intelligent locks and keys, each electronically enabled and unique in its identity. All CyberLock locks and keys are programmable and able to store critical information about their use and access privileges. As a consequence, management has very broad and flexible control over their pairing.

On the lock side, CyberLock now supplies over 420 different electronic cylinder types fitted with intelligent circuitry that controls access. Retrofitting to a CyberLock system becomes a simple matter of replacing existing mechanical cylinders, as opposed to replacing the entire lock. Each cylinder is energized upon contact with one of our battery-powered smart keys, which eliminates the need for expensive rewiring. The cylinders' rugged design makes them highly resistant to temperature extremes and tampering. Additionally, the sealed keyway prevents common lockpicking techniques.

On the key side, CyberLock's industry-leading range of smart keys combine portability and convenience with a host of programmable functions and data storage. Each has a unique ID code, which makes it easily traceable. It can retain a list of the locks it is authorized to open, store access schedules unique to that particular key, and identify the assigned user.

Maximum control with minimum effort

The other major component of the CyberLock solution is a diverse set of communication devices and software that bind the system into a networked whole. It enables administrative software, keys, and locks to exchange data in a way that gives management a wide variety of control options.

Ten different smart key designs give management the freedom to select the most efficient system configuration for their specific needs. Wireless-connected smart keys allow remote updating of targeted keys in the field, which can substantially reduce administrative overhead. Designated keyholders receive new access permissions without time-wasting return trips to the office. All the while, each key can continuously transmit an audit trail to a central location, where it can be used to trigger any number of management functions.

For instance, if a subcontractor's safety certification has expired, their key can be automatically deactivated until their certification is renewed, and then wirelessly reactivated. If a key is reported stolen, it can be permanently deactivated, thus avoiding the costly replacement of numerous locks. Also, each key can be programmed to adhere to a specific schedule that defines authorized access times.

A software solution that adapts to your specific organization.

When it comes to security management, no two organizations have identical needs. A state transportation department differs from a regional power utility, and so on. Accordingly, our CyberAudit-Web software offers maximum flexibility in how you manage the rich set of data produced by our smart keys. It readily adapts to almost any organizational setting, and integrates easily with other administrative software, such as Supervisory Control and Data Acquisition (SCADA) systems. And you can quickly configure it to meet any requirements posed by governmental compliance and accountability mandates.

Proper security for critical infrastructure is a complex undertaking. We're here to help.

CyberLock pioneered the electronic lock over 20 years ago and evolved it to its present state of sophistication. Along the way, we've accumulated a vast store of experience about what goes into a workable security solution in any given instance. Contact us and we'll put this knowledge to work on your behalf.

Designed, manufactured and assembled in the USA.