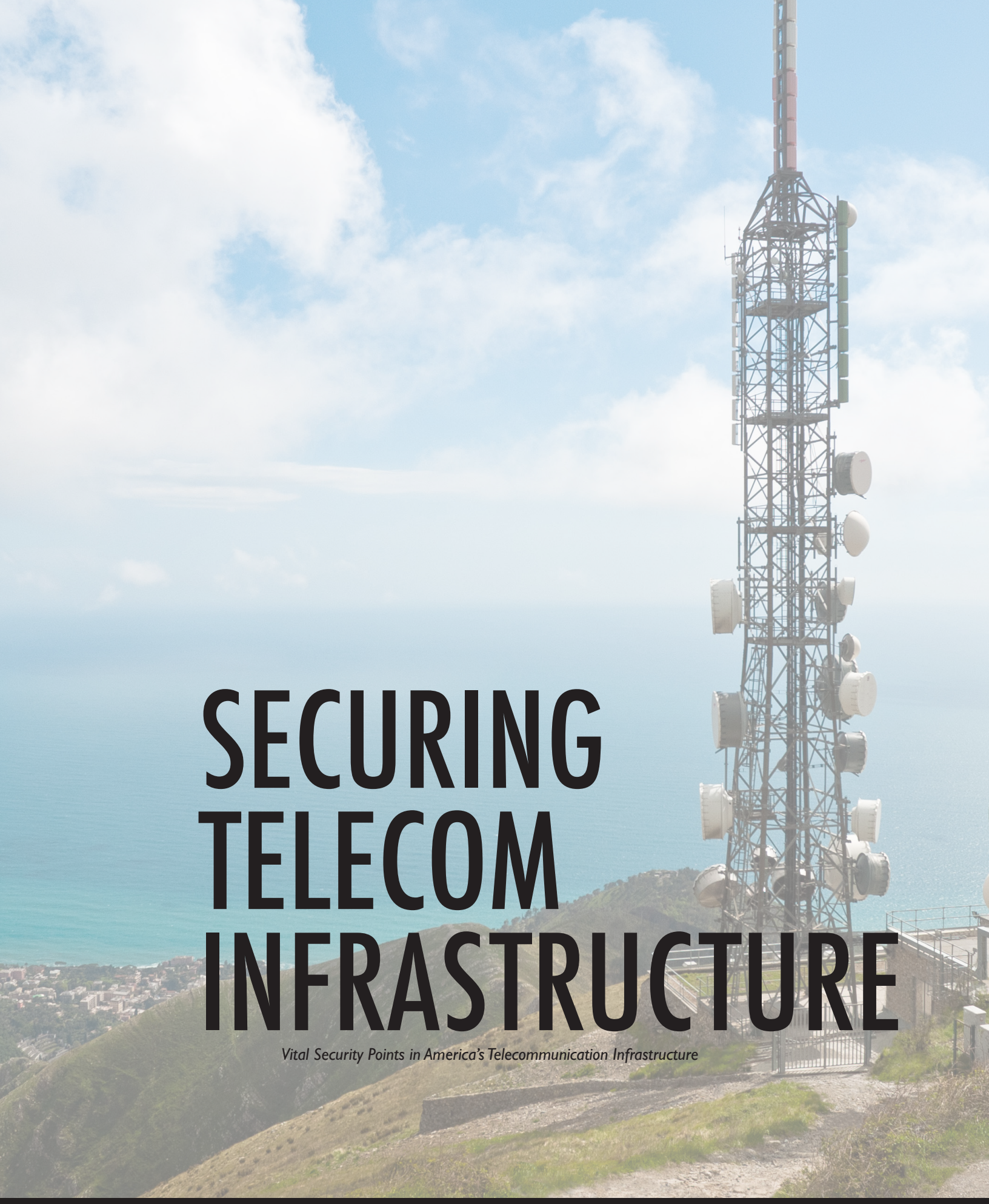
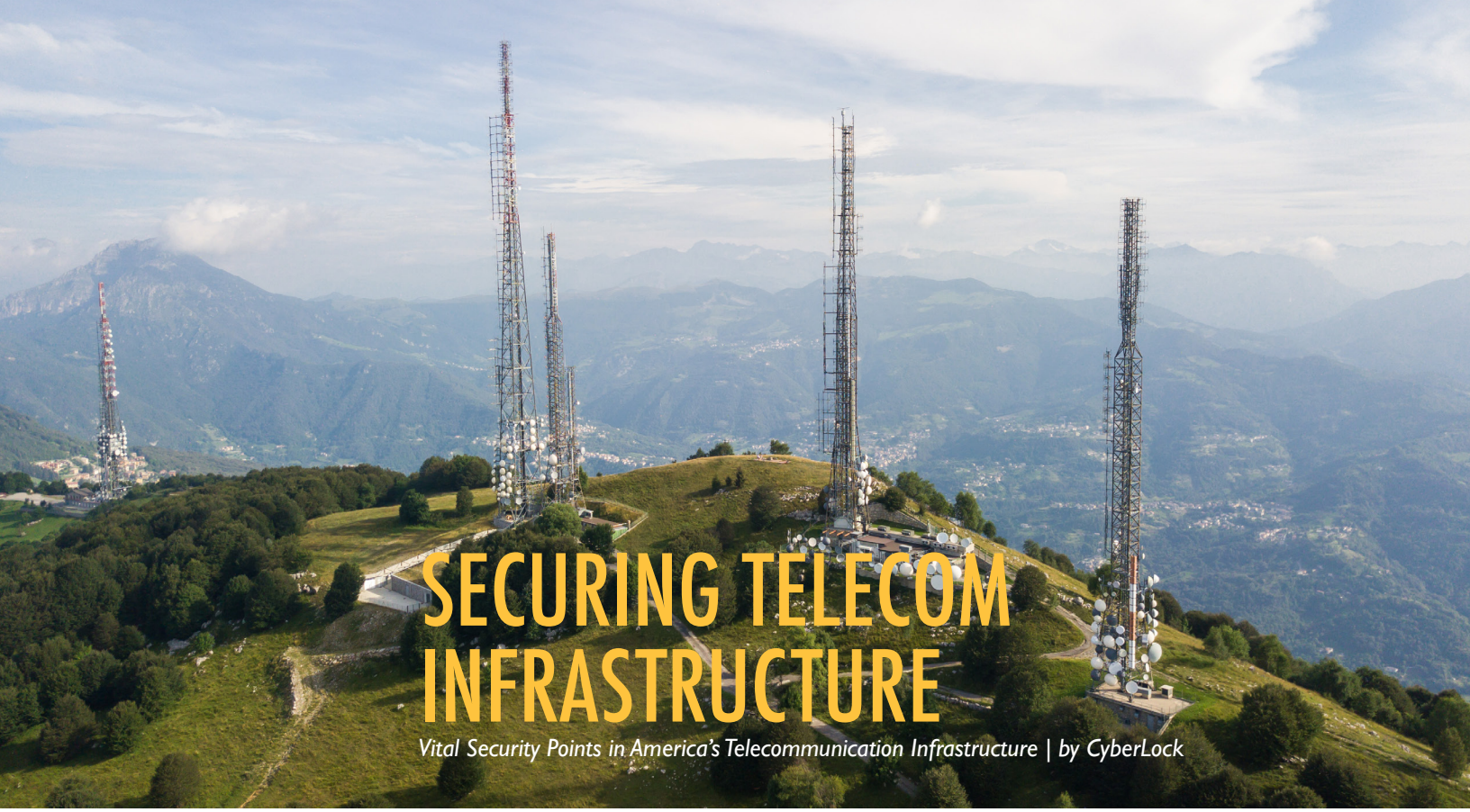


SECURING TELECOM INFRASTRUCTURE

Vital Security Points in America's Telecommunication Infrastructure

CyberLock®

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



SECURING TELECOM INFRASTRUCTURE

Vital Security Points in America's Telecommunication Infrastructure | by CyberLock

Persisting threats of terrorism and a succession of devastating hurricanes, tornadoes, floods, and fires emphasize our country's dependence on effective national telecommunication infrastructure. According to the Department of Homeland Security (DHS), there are 16 critical infrastructure sectors "that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety." Telecommunication is one of these 16 critical sectors identified by the DHS. Reliable, resilient communication services provide a vital bridge between emergency responders, firefighters, law enforcement, and civilians in times of emergency.

MANAGING WHO HAS ACCESS RIGHTS AND, PERHAPS MORE IMPORTANTLY, WHEN THEY EXERCISE THOSE RIGHTS IS ESSENTIAL TO MAINTAINING SECURE OPERATIONS.

Telecommunication companies face a number of security challenges that arise from their unique organizational structure. A reliable telecommunication network requires its wireless provider to operate an abundance of geographically widespread assets, frequently spanning multiple states. Moreover, many of these assets are remote, isolated infrastructure sites without onsite staff. To effectively administer this vast network of resources, wireless providers often have little choice but to rely on a complex web of dynamic work orders and rotating personnel. Managing who has access rights and, perhaps more importantly, when they exercise those rights is essential to maintaining secure operations.

Unique Problems of Telecom and the Failings of Mechanical Security

The myriad problems inherent in managing unstaffed, isolated sites regularly include vandalism and theft. Remote assets house expensive copper wiring, equipment rooms, and other valuable resources that are prime targets for thieves. While fences, locks, and alarms offer an essential layer of security, the easiest path for thieves to gain access to these assets is not through brute force, but through uncontrolled duplication of keys and operator negligence.

For telecommunication operators, the administrative headaches don't end with the thieves and vandals at their remote sites. Operators must monitor and control each site access from a revolving array of technicians, engineers, and maintenance personnel. As telecommunication technologies advance, personnel require access to a rapidly evolving labyrinth of equipment, from remote towers to densely deployed rooftop antennas. Wireless service providers often share different subdivisions within one site and each provider may have several employees or independent contractors coming and going, with little ability to control the scope of their movements.

OPERATORS MUST MONITOR AND CONTROL EACH SITE ACCESS FROM A REVOLVING ARRAY OF TECHNICIANS, ENGINEERS, AND MAINTENANCE PERSONNEL.

Mechanical locks and keys are generally the first line of defense when securing telecommunication infrastructure. With seemingly limitless variety, simple installation, and attractive prices, mechanical locks and keys offer an entry-level security solution. Although largely effective for basic needs, mechanical locks and keys can present serious risks for facilities that require a more sophisticated security system.

Audit Importance and Electronic Options

Notably, mechanical locks and key systems lack auditing capacity. In other words, the ability to track who was where, and when. Furthermore, the risks associated with lost, stolen, or copied keys are innumerable. With no way to effectively trace when a key is copied, facilities can easily lose control of the number of keys in circulation and, inevitably, their physical security altogether. Another troubling problem that telecommunication operators must confront is the variability in the type of locks used to secure gates, doors, and equipment rooms. With different manufacturers for each type of lock, keycontrol challenges can expand exponentially. Beyond fundamental key control problems, mechanical locks and keys are dangerously susceptible to picking and keyway vandalism, rendering the locks inoperable. Without the ability to precisely control keys and track personnel movement, mechanical locks and keys are simply not sophisticated enough for telecommunication security.

WITHOUT THE ABILITY TO PRECISELY CONTROL KEYS AND TRACK PERSONNEL MOVEMENT, MECHANICAL LOCKS AND KEYS ARE SIMPLY NOT SOPHISTICATED ENOUGH FOR TELECOM SECURITY.

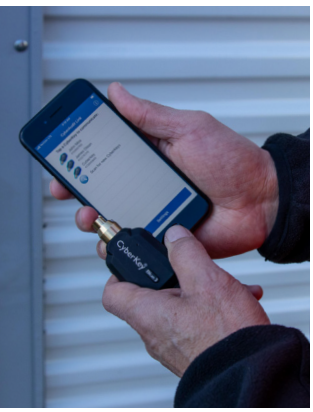
Electronic security systems, such as numeric pin pads, RFID card readers, and biometric devices, are commonly used in facilities requiring electronic tracking and precise, scheduled control over who is granted access. Although most electronic security systems provide enhanced security when compared to a mechanical solution, the installation costs, potential structural modifications, and power requirements are significant drawbacks. Electronic security systems require hardwired power and network connectivity, which is often unavailable or impractical at remote locations. Additionally, the cost and time associated with installing a hardwired access control system is notably higher than that of a mechanical lock and key system.

Closed circuit television and digital video security systems are another popular line of defense against vandalism, theft, and other security threats at telecommunication sites. Although cameras may present a deterrent for some thieves and vandals, they ultimately supply no physical protection to safeguard equipment and other valuable assets. Additionally, bandwidth limitations and data storage requirements may be unsuitable for the scattered nature of telecommunication infrastructure sites.

Key Centric Access Control

As telecommunication companies identify key control and audit capabilities as high priorities, one proven solution is CyberLock® electronic locks and programmable smart keys. Although less familiar than mechanical locks and keys, and perhaps even electronic security systems, key-centric access control systems combine the precision of electronic systems with the simple installation, affordability, and ease of use of a mechanical system. CyberLock access control systems bring full-featured access control to every locking

CyberLock solutions for remote access control



EACH LOCK AND KEY HOLD A MEMORY THAT RECORDS EVERY ACCESS ATTEMPT, ALLOWING MANAGEMENT TO VIEW A DETAILED AUDIT TRAIL SHOWING WHO ACCESSED, OR ATTEMPTED TO ACCESS, SPECIFIC LOCATIONS.

point without installing hardwired network or power connections. Electronic cylinders are easily deployed, not only on doors, but also on gates, trucks, shipping containers, and other mobile and remote assets. Because the cylinders quickly retrofit into mechanical hardware without power or wiring, installation is quick, easy, and affordable. Moreover, a proprietary sealed keyway prevents traditional picking techniques and guards against costly vandalism. The batteries in the CyberKey smart keys energize the CyberLock cylinders, meaning organizations don't need to manage expensive battery replacement schedules. In fact, CyberLock will continue to function during a power outage or emergency situation. Keys are programmed with access permissions for each individual user. If a key is lost, it can easily be deactivated in the system, completely eliminating the need to re-key. Each lock and key hold a memory that records every access attempt, allowing management to view a detailed audit trail showing who accessed, or attempted to access, specific locations. Key-centric access control provides the ideal security solution to meet the unique needs of telecommunication organizations.

Conclusion

Telecommunication infrastructure is vital to the security and safety of people worldwide. Securing remote assets as well as local sites can help ensure communication in times of emergency. Mechanical locks and keys and hardwired electronic access control systems have critical limitations. And, although helpful, cameras do not provide the necessary physical security barriers for a robust security system. With audit capabilities and precise key control forming the foundation of its system, CyberLock electronic cores and CyberKey smart keys are an excellent security solution for telecommunication infrastructure.

CyberLock®

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