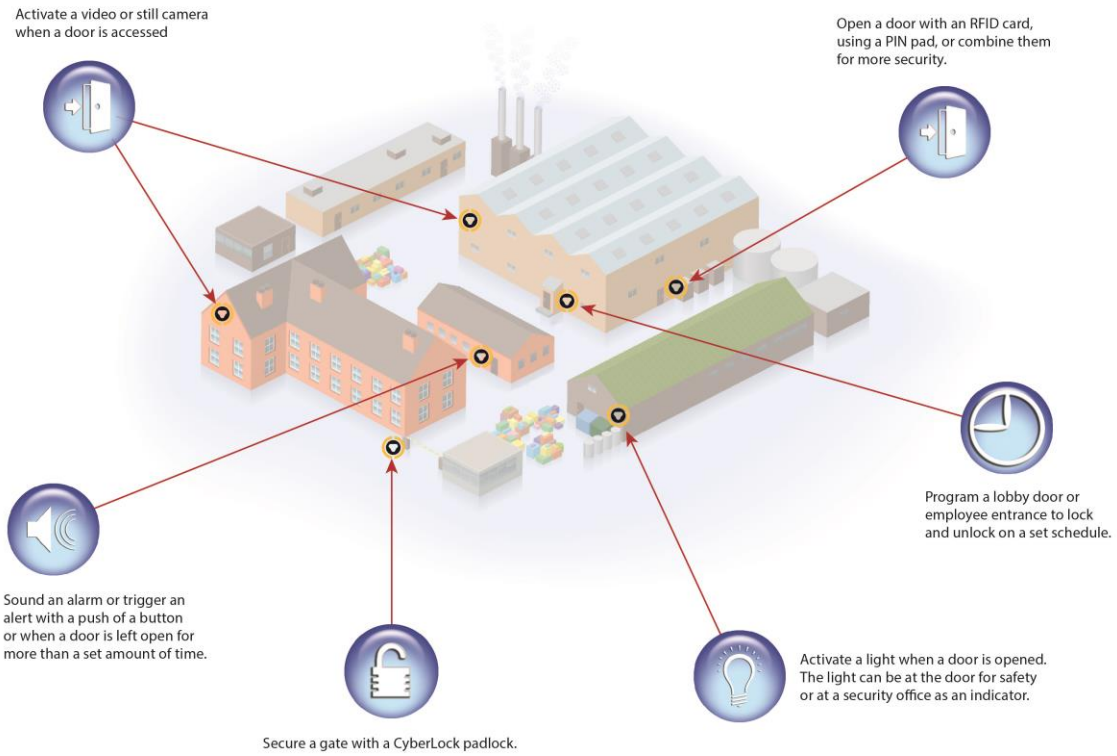
Securing Remote Access and Theft Prevention
By Kelsea McNutt and John Moa, Sales and Marketing, CyberLock

CHALLENGE: TSA regulatory requirements state that airport operators must show control of all the access points in their air operations area (AOA). For most airports, this means securing hundreds of remote access points and managing access for hundreds of key holders. Threats of insider theft by personnel add another layer of concern for airport operators. After 9/11, many airport systems were upgraded to increase security, but still for many, an update is crucial. An estimated shelf life of an access control system today is about 15 years old, with many airports utilizing systems over 25 years old.

When an airport ensures they are meeting regulatory requirements for access points like manual vehicle gates, it becomes critical for them to find a high security solution that can be integrated into existing card reader hardware. With dozens of miles of AOA restricted fence line, any hard-wired system would not be cost-effective. In Jeffrey Price's article titled, "It's Time to Upgrade the Airport Access Control and Badging System-What Questions Should I Ask?" published in *Observeit.com*, the Professor at the Metropolitan State University of Denver in the Department of Aviation and Aerospace states, "The insider threat to aviation continues to grow, with several recent airline bombings attributed to insiders. Airport Access Control and credentialing systems must become better at addressing the insider threat. Its not enough to know where an employee has access-today their access needs to be directly related to their work, with the ability to monitor certain activities, raising or lowering the level of authorization or access as necessary". He adds, "Using software that can both track, and restrict activity and access is one of the best practices that airport's should implement".

SOLUTION: The CyberLock Flex System is the only access control solution that offers both hardwired and key-centric technologies within one software package. With the Flex system, an airport can keep their existing card reader hardware, while also securing hundreds of remote access points with CyberLock padlocks. The Flex System is comprised of a variety of modules that can be mixed and matched to create a custom access control system. The modules are plugged into a Hub, which is directly connected to CyberAudit management software. The Flex System Hub connects with CyberAudit software and provides power to the Flex System modules. Embedded memory in the Hub stores access permissions and saves audit trail information, enabling continuous operation even when a network connection to the software is interrupted. Moreover; connecting a back up battery or auxiliary power source directly to the Hub can mitigate power outages. For this customized access control system, there are many modules available. Input modules such as RFID readers and Keypad Displays can be used individually or combined for dual-credential door access. Also, weather resistant key vault modules can be installed in the field to securely store CyberKey smart keys for convenient remote employee

access. The Flex System also has door and I/O Modules. This module expands the capabilities of the Flex System even further. As a door controller, it provides power to an electric door strike and unlocks it when an approved key card is presented. It has additional inputs and outputs that can control relay devices such as alarms, speakers, cameras, or sensors. Finally, it can connect to compatible third party Wiegand devices such as HID readers and biometric scanners.



REMOTE ACCESS IN ACTION

One security administrator at an international airport in the southern US gave 251 maintenance workers, police, fire fighters, guards and FAA employees CyberKeys with short expirations. This gave them increased key control by requiring employees to update their keys often. This also added an additional layer of theft prevention by utilizing short access permissions to make it difficult for keys to be passed around to employees who should not have access to restricted areas.

Airport Security Administrators now have the ability to view reports that show who accessed specific vehicle gates and remote areas, keeping them compliant with TSA regulatory requirements. The CyberLock Flex System can give them this ability without having to change the access control system they already have in place and without hard-wiring miles of remote access points, saving a great deal of time and money.

The 10th largest airport in Australia, serving in excess of 2 million passengers every year, shares runways with the Royal Australian Air Force's RAAF Base. The airport terminal is utilized for both international and domestic flights, with separate cargo handling facilities. The site also supports a number of retail outlets and cafeterias. As with all airports, the AOA covers a considerable area and many of the sites can be remote. Overcoming the challenges of distance was a key aspect of this access control installation. They needed a security solution to stand up to the rigors of an airport environment and work within a very complex system requiring authorization entry at different levels within the airport. The system had to work in the humid air and not interfere with the high-powered two-way radio and radar emissions that surround the airport. CyberLock's system could solve this problem.

After bench testing the concept, a key and key authorizer was sent to communicate with the company's server in Sydney in real time. Once this part of the puzzle was confirmed, they accepted the concept and had solar units built and erected, ready for deployment when the installation team arrived. The programmability of the CyberLock system allows the airport to control the challenges of distance. Lost or stolen keys can be easily blocked, access to locks can be individually programmed into each person's key, a complete audit trail from the key and the lock can be retrieved, and a single key can be used to open all different types of locks at the airport. To obtain such controls, the nucleus of the CyberLock system is the Enterprise server. This is where traditional access rights are determined such as door lists, people lists, time schedules, access matrix, and location graphics. The database was installed on a HP server using a Linux operating system. The information from the database was transmitted to the key update authorizers using TCP/IP protocols. In the terminals, this transmission is over Ethernet cabling, but on the perimeter of the airport in remote locations where cabling could not be achieved, the 3G network was used for the communication between the server and the key updating authorizers.

Today, overcoming the challenge of distance is not a problem for airports using CyberLock. They now have the ability to monitor all access points, even remote locations, which has increased their security to the highest level. The CyberLock system gives them the ability to review reports that show who has accessed specific gates and remote areas, increasing their security and monitoring all action around the AOA. This in turn helps airports stay on top of any potential security issues that may arise, so quick action can be taken.