How can electromechanical keys help enforce security and compliance in critical infrastructure?

The ever expanding private and public infrastructure is ultimately changing the landscape of how we communicate and access services across vast geographical locations. With the modernisation of our critical infrastructure technology comes great benefits to our lives including the ability to work from anywhere. The danger or risk of disruption to our businesses should a critical infrastructure site such as public safety networks, water networks, power infrastructure, or even telecommunications towers go down or worse, be compromised by a physical security flaw, that is, an unauthorised user gaining access, is very real.

With COVID-19 having such a global impact on our country's decision makers, we must never forget there are other real dangers that exist such as natural disasters and terrorism. Having a weak link in the security chain means organisations are potentially exposing themselves to unauthorised access and an increased level of risk.

The myriad of challenges inherent in managing unstaffed, typically isolated, or remote sites include vandalism, theft (both external and internal), or even an 'influencer' producing the latest trending video or post on popular social media platforms. Additionally, remote assets house expensive wiring, batteries, equipment, and other valuable resources. While fences, locks, and alarms offer an essential layer of security, the easiest path for intruders to gain access is not through brute force, but through either their normal mechanical key, an uncontrolled duplication of mechanical keys, an authorised user not locking up as per their procedure, or even negligence.

For critical infrastructure operators, the administrative headaches do not end with would be intruders. Operators must monitor and control each site access from a revolving array of technicians, engineers, maintenance personnel, and contractors. For example, 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. These workers range from gardeners to technicians and in many cases the technicians are contractors who have a key to the gate, and then Telco 1 Key, Telco 2 Key, and Telco 3 Key, to access the various subdivisions within the site. The site owner typically leases space to the different site users, but their security is only the start of the challenges. Of greater concern is an unapproved person climbing the tower which presents even greater risks.

Mechanical locks are generally the first line of defence when securing critical infrastructure sites. Although largely effective, mechanical locks and keys can present serious risks for facilities that require a more sophisticated security system, notably a lack of audit trail and the fact that the system is virtually 100% redundant as soon as the first key is lost.

Ensuring that authorised personnel only have access to critical infrastructure such as emergency services or a public safety network site is paramount to keeping people and places safe, not to mention minimising any public liability damages due to non-controlled access. In many cases, these sites are in regional or remote areas, and having the right enterprise access control that is both cable free and does not rely on batteries or power in the locks but can still offer virtual real time access with complete audit trails and integration with the induction and compliance system is key to maintaining control.

On the surface, access permissions based on a mechanical key system to restricted sites seems straight forward. A maintenance employee or an independent contractor has a specific restricted key that can access specific locks, therefore can access a site to do a routine job. What lies below the surface is currently shaping the future of site access security.

To get in to this a bit more, let's explore further;

1. Can this employee or contractor show they were at the site at the time they stated?
2. Did they complete the job at the time they stated?
3. Did they lock the padlock and gate after finishing the job? (Note, many remote sites utilise padlocks for entry)
4. Are the contractor's public liability insurances up to date?
5. Is there a thunderstorm or heavy rain heading over that site at the same time the job is to be scheduled?
6. Has the employee or contractor attended the latest Work Health and Safety training program?
7. Has a work permit been obtained before accessing the site?

All these are valid questions. Let us paint a real scenario

- An independent contractor, let us call him Jim, has been asked to go to a water reservoir (this could of course be a communications tower or electrical substation) that is 80KM outside of the Sydney CBD.
- On their way, it begins to rain and as Jim approaches the tower there are now thunderstorms.
- As part of the company Jim contracts to, it is required he attends a WHS webinar once per quarter. Jim missed the last WHS session.
- Jim also realised that on the way to the job he had forgotten to renew his public liability insurance.

To surmise, Jim is going to a job with potentially dangerous weather conditions, has not attended recent WHS training, and his insurance has expired.

The HR implications alone in the above scenario if anything were to happen to Jim is enough to produce many sleepless nights for any CEO, Business Unit Manager, or Risk Manager.

What we are seeing and developing with our EKA CyberLock platform is a complete holistic 360-degree view of an employee or contractor working on these types of sites. One of our major customers who has installed EKA CyberLock on over 395 sites with over 1,800 padlocks spread at remote sites across Australia, has recently integrated their systems by giving access permissions to a contractor's CyberKey based on this said contractor compliance and induction status. Before access is granted the system checks,

- Insurance is current,
- The weather is safe to work,
- Has site induction been completed,
- If any of these or other required factors are not up to date, then access to a CyberKey is not granted.

EKA CyberLock has been providing access control for padlocks and all types of locking devices in remote sites with no power or batteries and a complete audit trail for over 20 years. We are the leaders in electro-mechanical technology, just ask us and we can give you names and numbers of customer reference sites in the Government, Utility, Telco, and Education sectors (plus more).

Providing leading edge electro-mechanical keys systems for securing critical infrastructure sites gives back control to manage access to remote sites in the same way as they would manage access to the front door of their head office. Now however, the landscape has changed with EKA CyberLock using security to shape company policy by developing integrations between CyberLock Software and staff/contractor compliance and inductions systems.

Written by: Geoff Plummer
Executive Business Manager
DAVCOR Group Pty Ltd
www.ekacyberlock.com.au I 1300 722 311
in www.linkedin.com/in/geoffplummer