How Security Shapes Policy

The ever-expanding communication towers and repeaters bolstering our latest 5G network continues at remarkable speeds in terms of new builds by the Telcos and not to mention my download speeds of 900MB/S. This is ultimately changing the landscape of how we communicate and how accessible we are in many geographical locations. With these great benefits to our lives including the ability to work from anywhere, comes the huge risk of disruption to our businesses should a 5G tower go 'down' or worse be compromised by a physical security flaw, that is, an unauthorised user gaining access to a tower. In many cases, these towers are in regional or remote areas and are very prone to attack. The aim is to not only secure the tower but also control authorised access.

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 to not only telco towers, but public safety sites, high voltage power areas, dams, and many more places that are classified as critical infrastructure.

The myriad of challenges inherent in managing unstaffed, typically isolated, or remote sites regularly 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 contractors range from gardeners to technicians and in many cases the technicians are contractors who have a key to the gate, and then a Telco 1 Key, Telco 2 Key, and Telco 3 Key, to the various subdivisions within the site. The site owner is more concerned about unauthorised access to climb the tower without the safety approval and training.

Mechanical locks are generally the first line of defence when securing telecommunication towers and critical infrastructure. 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 redundant as soon as the first key is lost.

Ensuring that authorised personnel only have access to critical infrastructure sites is paramount to keeping people and places safe, not to mention minimising any public liability damages due to non-controlled areas. In many cases, like telecommunication towers, 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 or even WiFi but can 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? Did they complete the job at the time they stated?
2. Did they lock the padlock and gate after finishing the job? (note many remote sites utilise padlocks for entry)
3. Are the contractor's public liability insurances up to date?
4. Is there a thunderstorm or heavy rain heading over that site at the same time the job is to be scheduled?
5. Has the employee or contractor attended the latest Work Health and Safety training program?

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 communications tower that is 300KM outside of the Sydney CBD. On his 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 in this industry.

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 all across Australia, has recently integrated giving access permissions to a contractor's CyberKey based on this said contractor insurance is current, the weather is safe to work in, and they have passed their WHS certifications. This site access software covers WHS, compliance, induction, and ensures insurances are updated. 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 to padlocks and all types of locking devices in critical infrastructure 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 Utility, Telco, Government, and Education sectors (plus more). However, developing integrations with other software systems that allows administrators automated full control while maximising safety and risk managing WHS claims is where we are changing the security landscape that will benefit Critical Infrastructure by providing productivity and safety gains to streamline processes across these organisations.

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