THE ROLE OF LOCK SYSTEMS IN **PROTECTING** OUR NATIONS CRITICAL INFRASTRUCTURE

NEXT GENERATION WIRELESS ELECTRONIC LOCKING
to secure utilities, facilities, remote sites, data centres, education, intelligent transport systems and more.

THE ROLE OF LOCK SYSTEMS IN PROTECTING OUR NATIONS 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 centre 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 behaviours are an enduring fact of life. And so it is that security measures have become a permanent fixture in modern organisations at nearly every scale, from global transport to local wastewater treatment.

Security is a multi-dimensional challenge.

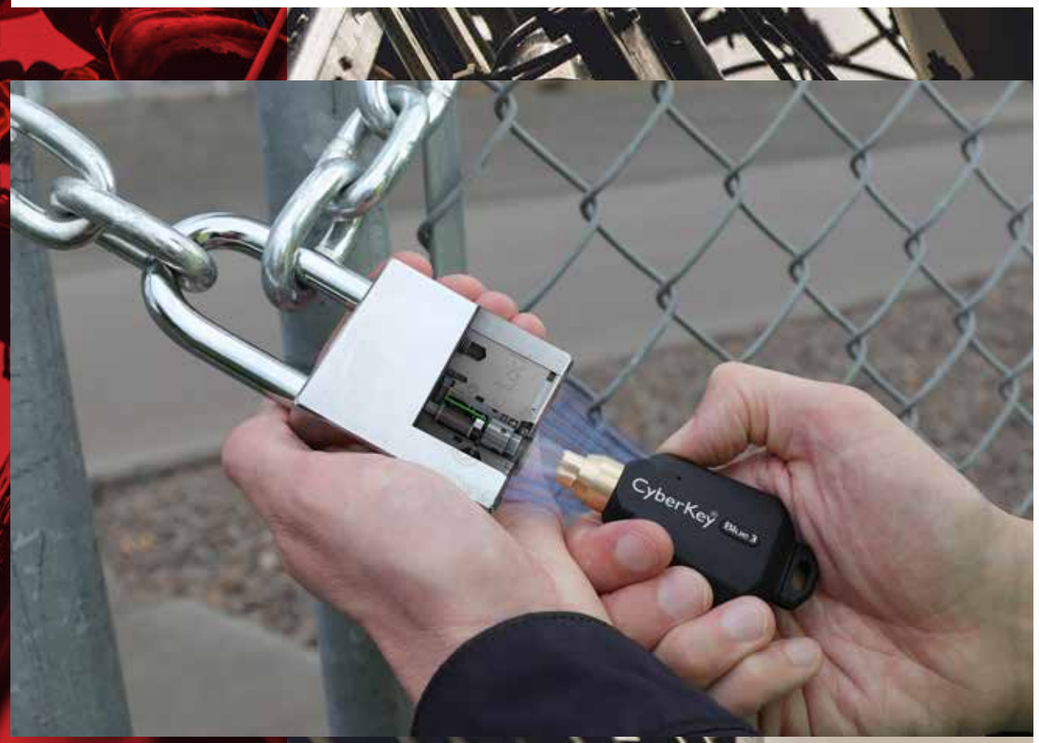
In recent times, security management largely concerned itself with the physical aspects of asset protection. Locks, doors, cabinets, gates, and other such barriers formed the basic core.

However, the complexity of modern organisations has introduced a new set of challenges centred 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, safety, 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 organisations efficiency and productivity.

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 organisations 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 their 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 specialised solutions.

Physical proximity plays an important role in an organisations 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. In many cases, these sites rely on conventional mechanical locks to secure critical access areas, such as towers, gates, water boards, hatches, pits, server racks, traffic control cabinets, re-pumping stations and chemical feed stations, just to name a few.

The myriad of challenges inherent in managing unstaffed, typically isolated, or remote sites regularly include vandalism and theft (both external and internal). 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.

These mechanical locking systems also present numerous administrative challenges. Conventional keys are untraceable and if they are out of patent can be easily duplicated. Key registers, signing keys in and out, following up non-returned keys, and coupled with monthly or quarterly key audits to ensure the health of a mechanical master key system is an administrative burden, but must be done to ensure how many keys are in service and more importantly, who they're assigned to and how many may be compromised.

In many instances, keys may remain in circulation even after their owners no longer have access privileges, opening the possibility of malicious behaviour. Consider the case of a subcontractor who fails to turn in their key and cannot be contacted. Now depending on the level of this master key, will determine how many cylinders and keys will need to be replaced - a painful but sometimes necessary solution.

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. For example, in the utilities sector that have sites in regional or remote areas, having the right enterprise access control that is cable free, does not rely on batteries, power or Wi-Fi in the locks, can offer virtual real time access with complete audit trails, and provides the capabilities for integration with various other systems such as an induction and compliance system, is key to maintaining control.

At EKA CyberLock all locks are not created equal – by design.

An EKA CyberLock IP68 padlock securing a major utility in regional NSW.

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

On the lock side, EKA CyberLock now supplies over 370 different electronic cylinder types fitted with intelligent circuitry that controls access. Retrofitting to a EKA CyberLock system becomes a simple matter of replacing existing mechanical cylinders, as opposed to replacing the entire lock. Each cylinder is energised 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 – they can operate from -40°C to 70°C.

These extreme temperatures are never going to occur in an office building, so how do you put a form of access control on a padlock that has no power, network, cabling, or even Wi-Fi around it? Well, padlocks provide the physical locking for a large percentage of remote assets. This means having an "Australian Proof" padlock solution that is strong, solid, durable, and dust, salt, sand and water-resistant which are minimum requirements to handle our environment is a must. EKA CyberLock have a vast range of padlocks suitable for any application, all of which can be fitted with an IP68 electronic EKA CyberLock cylinder, thus expanding your electro-mechanical key system to assets in remote sites.

On the key side, EKA CyberLock's industry-leading range of smart keys known as, CyberKeys, 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 authorised to open, store access schedules unique to that particular key, and identify the assigned user. The latest CyberKey Blue3 is RoHS compliant and can easily update access privileges to a user via its connection to an app on a phone which in turn connects to the management software, typically hosted in a cloud environment.

Like many services orientated managers considering an electro-mechanical solution, the thought of the cost of replacing batteries in a large number of electronic cylinders or locks (for example 1,000 cylinders) located on a large site such as an education facility every 12 months can be very confronting. Well, imagine the additional cost in labour and time if these were securing the assets of a major utility spread over a huge geographical area such as an entire state. EKA CyberLock cylinders and padlocks have no batteries in them and are powered by the battery in the CyberKey. This key battery is normally rechargeable even in the car, meaning the cost associated with visiting locks and replacing batteries is eliminated.

Maximum control with minimum effort.

The other major component of the EKA 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 CyberKey designs give management the freedom to select the most efficient system configuration for their specific needs. Bluetooth enabled smart keys allow remote updating of access profiles in the field (via a mobile phone app), 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 transmit an audit trail to a central location, where it can be used to trigger any number of management functions, processes, audits, and reports.

For instance, if a subcontractor's safety certification has expired, their CyberKey can be automatically deactivated until their certification is renewed, and then wirelessly reactivated. If a CyberKey is reported stolen, it can be permanently deactivated, thus avoiding the costly replacement of numerous locks (refer to ***Remote sites pose unique vulnerabilities that require specialised solutions*** section above). Also, each key can be programmed to adhere to a specific schedule that defines authorised access times.

A software solution that adapts to your specific organisation.

When it comes to security management, no two organisations 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 organisational setting, and integrates easily with other administrative software, such as security, WHS, induction and compliance 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 are here to help.

EKA CyberLock pioneered the electronic lock over 20 years ago and evolved it to its present state of sophistication. Along the way, we have accumulated a vast store of experience about what goes into a workable electro-mechanical master key system in any given instance. Contact us and we will put this knowledge to work on your behalf.

CONTACT US

SYDNEY • MELBOURNE • BRISBANE • PERTH • ADELAIDE • AUCKLAND

1300 722 311
WWW.EKACYBERLOCK.COM.AU

+64 (0) 9 368 4802
WWW.EKACYBERLOCK.CO.NZ

V.1.0-2108 | EKA CYBERLOCK DIVISION OF DAVCOR GROUP PTY LTD