princeton IDENTITY

PROTECTING MISSION CRITICAL INFRASTRUCTURE WITHIN COMMERCIAL PROPERTIES SHOULD BEGIN WITH BIOMETRICS

When tenants sign a lease, they trust the building's management to maintain the property's critical infrastructure. Electrical, heating, ventilation, water supply: these systems are mission-critical. Their failure can temporarily shut down a building, causing inconveniences and financial losses for occupying tenants. In some instances, the impact can be catastrophic.

Protecting such systems from tampering or outright attack requires the highest levels of security. Proximity to equipment must be tightly regulated, as well as network access to software vital to their management and operation.

There is no better tool than biometrics to secure access to these assets. It is easy to layer biometric identity systems on top of technology already in place, creating multi-factor authentication solutions that are practically impenetrable.

Let's start with physical access control. At any commercial property, doors to boiler rooms, system headends, telecommunication centers, utility closets, and other critical infrastructure should already be protected by highly secure electronic access systems. Authorized facility management, maintenance personnel, and contractors must have special credentials to enter these areas. However, PIN codes can be shared and cards can be stolen or cloned. A superior solution requires workers presenting a credential to physically match the authorized cardholder's biometric data – a digitized, encrypted reading of their iris, face, palm, or fingerprint. This is a requirement nearly impossible to fake. For example, the probability that an iris biometric would register a false match is less than once in one million.

Biometrics can be implemented in one of two ways. A database can store encrypted codes representing each enrollee's biometric signature, or the biometric data can be stored on each individual's access control card. Today's 13.56 MHZ smart cards feature programmable memory designed for these types of applications. Adding a biometric layer to identity verification is so effective that Homeland Security recommends it be part of any multi-factor authentication system for access to Federal government locations.[1]
While no such directive exists for commercial properties, shouldn't tenants feel similarly confident that their workplace infrastructure is well protected?

[1] https://csrc.nist.gov/publications/detail/sp/800-76/2/final

Of course, any conversation about securing infrastructure would be incomplete without addressing network security. Controlling physical access to datacenters can be accomplished with biometrics; the same technology can be applied for logical access to the network itself.

Traditionally, the most sensitive network management permissions were granted only to workers located physically within a datacenter. The pandemic introduced the need for some of these employees to work remotely and, with it, fail-safe methods to authenticate and verify their identity. Combining biometrics with passwords allows networks to validate each user's identity as they sit at their computer, regardless of where they're located. Leveraging a computer's embedded camera or attaching an encrypted biometric reader to verify the user's face or iris, the user's identity can be repeatedly matched against their enrolled biometric data. If someone replaces or joins them in front of the monitor, the application or the computer will immediately shut down.

In addition to enhancing security, this solution can deliver economies of scale for management firms with multiple, disparate holdings. A centralized critical IT support team can provide remote maintenance and system updates to an entire portfolio of properties. Biometric identity solutions, combined with zero trust architecture and other technology like computer privacy screens, remove any distinction between the security implications of working onsite versus remotely.

Commercial real estate may not be ready to implement biometrics on a wide scale just yet. Its use requires buy-in from everyone who will use the system – a tough challenge in multi-tenant properties with many different stakeholders. However, the decision to use biometrics to secure a buildings' critical infrastructure poses few such obstacles, with benefits far outweighing installation and start-up costs. Building management controls and manages those assets. They, alone, have the power and responsibility to do whatever it takes to keep them safe. Implementing biometric identity solutions is the place to start.