Introduction

Whether you're a large corporation, small company, organization or government agency – a security breach can deal crippling damage to one's brand and reputation, as well as leave consumers as prey to scenarios like identity theft, virtual robbery or even physical injury. Yet despite new technology, protocols and security best practices, breaches – both virtual and physical – are an all-too-common scenario.

Here are some new axioms, best practices and technology capabilities that will act as drivers to improving access control in the immediate future and become the standard in the coming years.

Source: Michael Elias

http://www.securityinfowatch.com/article/12409842/6-methods-to-- enhance-your-facilitys-access-control

1. Security is Not Limited to the Front Door

Security must encompass more than the front door: Most security checkpoints are located just beyond the front entrance. But today's solutions also need to track what's happening once an employee is inside. To effectively enhance security, we need to know who is doing what, where and when at all times. Ignorance isn't bliss, and it can quickly leave you maimed if you're not careful.

2. Solving lost and stolen badges

Human error can quickly lead to a large break-in if just a single badge is misplaced or stolen. And the RFID badge system is riddled with flaws. In 2015, for example, more than 1,400 security badges went missing from Atlanta's Hartsfield-Jackson International Airport, which could grant access to private baggage areas, tarmacs and other secure locations. Even if they're not physically stolen, most RFID badges can be quickly cloned undetected by the user. Eliminating this challenge requires more than a simple PIN number – we need multiple authentication methods that cannot be counterfeited..

3. Eliminating badge abuse

We like to believe that an employee won't abuse their badge and security clearance – but all it takes is one rotten apple to spoil the whole bunch. A unique PIN can be assigned to prevent the use of stolen badges, but what if an insider decides to sell that information? There are several ways to be nearly 100 percent sure the person opening the door is who they say they are – and they don't require implants.

Biometric authentication – such as retina, fingerprint or facial recognition – is just one way to prevent this type of badge abuse.

Advanced Access Control
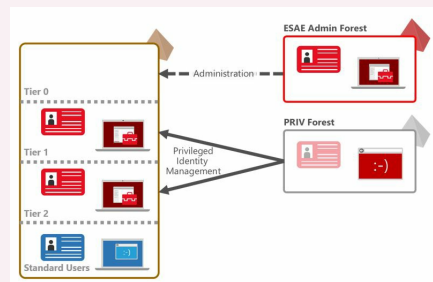
4. Preventing tailgating and piggybacking

A badge system can prohibit an intruder from entering, but not if someone on the inside opens the door first. These types of scenarios happen all the time – both intentionally and unintentionally – and leave otherwise highly secured areas extremely vulnerable. To solve this, it's not enough to just know who scanned the badge – we need to know who (and how many) actually entered with them.

5. Improving emergency response

Unfortunately, the need for emergency response has become an all too common occurrence. And response times have a direct correlation to the severity of damage from a breach. Systems today lack the most critical feature to improving response time – which is identifying and relaying the exact location of the emergency.

First responders would benefit greatly if they could verify the authenticity and exact location of an emergency at any time. It's not enough to know which building, but rather which room and which level.

6. Building business intelligence

For good reason, our world is becoming more and more data driven. And by improving the way we monitor employees and access control, we can unlock a huge stream of untapped information. These insights could range from better understanding the routines and processes of staff to improve productivity, to better identifying threats and breaches before they have a chance to strike.