VANDERBILT

News

Three Reasons Why Organizations Should Ensure Access Control Technology Is Up to Date

When it comes to the technology we use in our daily lives, updates and upgrades are seemingly instinctual. If a new version of the iOS software for iPhones becomes available, for example, we download and install it within days — or even hours. When our laptops or computers start to slow down and become incapable of running the latest and safest software, we invest in a new device because it's worth the long-term gain.

Because this process comes naturally to us, you'd expect the same would be the case when it comes to technology upgrades in the security industry. But oftentimes, organizations fall behind, especially when it comes to access control. Many traditional management personnel consider an access control purchase a one-time investment, which

may lead to the use of 10- to 15-year-old systems. Relying on outdated technology like this can create numerous challenges and should be avoided for the following reasons:

Cybersecurity Concerns

The goal of an access control system is to purposefully manage access to specific areas to protect personnel and property, but when the technology being used is antiquated, organizations increase the risk for breaches to occur. Older technology likely does not have updated network security features in place, making it open to being compromised and potentially granting unauthorized access to both the facility itself and its network. From a cybersecurity perspective, a solution that is connected to the cloud but doesn't possess the proper encryption and password protections is left open to risk. Additionally, when software updates and patches are not installed in a timely manner, the system becomes vulnerable to weak points and the enterprise's overall system is put in jeopardy.

Lack of Interoperability

Legacy access control systems were created with one goal in mind. But in today's evolving and complicated risk landscape, organizations are looking to integrate their security technology to create a single, streamlined platform that addresses more than one area of concern. Collaboration and interoperability are key in achieving this goal, which can be hard to establish with outdated technology. Obsolete access control solutions traditionally cannot communicate with other systems and therefore cause data to be siloed and incident response to be uninformed.

Lack of Innovation

If a business is running an older access control system, they're likely missing out on the latest innovative technologies that are available for enhancing the solution. There are several options available when it comes to selecting the right security system and platform for a business. Some might prefer an on-premise solution, while others find the benefits of a cloud-based system more suitable for their day-to-day operations. Between remote monitoring, central management, simplified lockdowns and more, both are viable options for an updated solution. Technologies such as artificial intelligence (AI), video analytics and

building management systems are also easier to incorporate into a modern access control system.

The bottom line is: Technology is always changing. And when it comes to security, falling behind can lead to detrimental consequences. For an access control system to function properly without creating any unwanted issues, it's in an organization's best interest to stay up-to-date with the latest software and hardware enhancements. Doing so can lead to both safer systems and added functionality for improved operations.

Browse through our Access Control portfolio today!