# Key Indicators Suggest Need for Access Control System Upgrades, Says Don Tucker of D&D Audio and Video Solutions

SLIDELL, LA, UNITED STATES, July 31, 2025 /EINPresswire.com/ -- Aging access control systems in commercial and residential settings may expose properties to unnecessary risk. As criminal tactics evolve and technology advances, certain warning signs suggest that an upgrade to an access control system may be overdue. Identifying these issues early can help reduce the likelihood of unauthorized entry, operational downtime, and compliance failures.
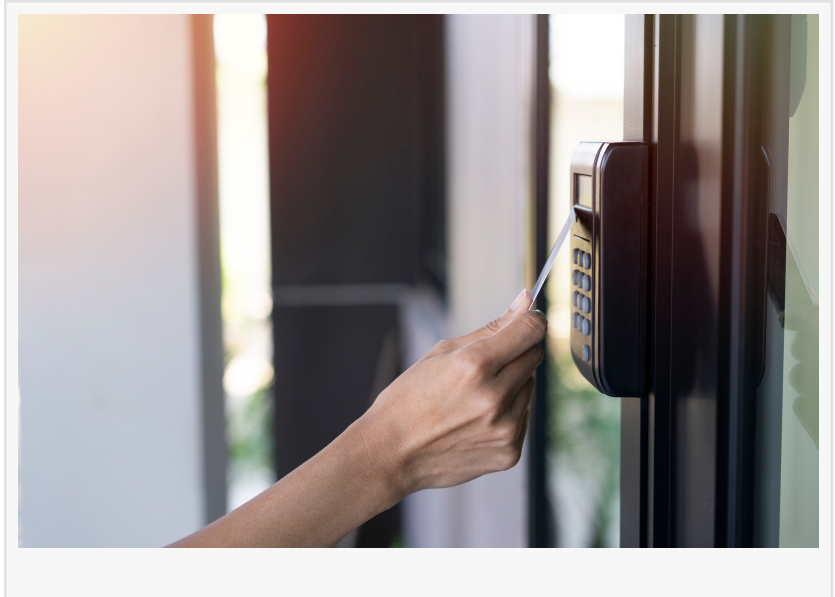
Frequent System Malfunctions

Doors that don't unlock on the first try, delayed responses to badge scans, or readers that stop working altogether often indicate a system under strain. Whether caused by outdated hardware or environmental degradation, repeated malfunctions point to diminishing reliability. If a system fails more than a few times a year, replacement parts or manufacturer support may no longer be available—leaving the property vulnerable.

> Access control systems were once seen as a set-it-and-forget-it investment, but evolving needs and threats demand ongoing reassessment"
>
> *Don Tucker*

Limited Remote Management Capabilities

Today's systems often allow administrators to manage users, review access logs, and schedule lockdowns from anywhere. Without these capabilities, teams must operate onsite, increasing response times and creating workflow disruptions. The absence of real-time remote access limits visibility and slows down decision-making during incidents.

Lack of Integration with Other Security Systems

Modern building security relies on connected systems. Access control platforms are expected to

interface with fire alarms, intrusion detection, and emergency alert systems. For example, if a fire alarm triggers, doors should unlock automatically to allow safe evacuation. Older systems may not offer such integration, creating gaps in building safety protocols.

Weak or Missing Audit Trails
Access logs are critical in the aftermath of an incident. Systems that fail to record who entered, when, and where—especially if logs are limited or overwritten too quickly—make it difficult to identify liability or confirm compliance. Regulatory bodies and insurance providers increasingly expect access control systems to produce detailed, reliable records.

Credential Management Limitations
If lost badges or credentials remain active and cannot be promptly deactivated, the risk of unauthorized access grows. Legacy systems often lack the ability to set expiration dates or issue time-restricted access. Newer systems offer more sophisticated options, such as one-time codes or mobile credentialing, which reduce reliance on physical keycards altogether.

Obsolete Encryption Protocols
Access control no longer deals solely with doors and gates—it plays a key role in cybersecurity. Many older platforms use outdated encryption, leaving the system vulnerable to attacks that could compromise both physical and digital networks. Upgrading to systems with current encryption standards strengthens overall infrastructure.

Inflexibility During Expansion
When businesses add entry points—like new gates, back doors, or warehouse bays—some older systems can't easily scale. A limited number of reader connections or a closed software environment can force a complete system overhaul instead of a simple expansion. Scalable systems reduce this friction and make future growth more efficient.

Failure to Meet Regulatory Requirements
Industries such as healthcare, education, and finance must adhere to specific standards, including HIPAA, FERPA, and SOC 2. These regulations may dictate how access data is stored, who can access it, and how it must be reported. Systems that cannot meet these benchmarks risk non-compliance and potential penalties.

No Support for Mobile Credentials
Mobile access credentials—such as Bluetooth, NFC, or QR-based entry—are quickly becoming standard in modern workplaces. Systems that don't support mobile access limit user convenience and hinder advancements in security like multi-factor authentication and

temporary guest access.

End of Vendor Support or Software Updates
Manufacturers eventually end support for aging systems. Without software patches or hardware replacements, systems become more prone to failure and increasingly incompatible with other technologies. Continuing to operate unsupported access control platforms increases the chance of a critical breakdown at the worst possible time.

Quote from Don Tucker
"Access control systems were once seen as a set-it-and-forget-it investment, but evolving needs and threats demand ongoing reassessment," said Don Tucker, owner of D&D Audio and Video Solutions in Slidell. "Failure to act on these warning signs can lead to vulnerabilities that compromise both physical and digital security."

About D&D Audio and Video Solutions
D&D Audio and Video Solutions is based in Slidell, Louisiana and serves clients throughout the Gulf States. The company focuses on custom installations of advanced access control, automation, and audio systems for residential and commercial properties. Owner Don Tucker brings decades of hands-on experience in system design, integration, and lifecycle management. The company also offers professional installation of Crestron home automation systems, with deep knowledge of whole-home control for lighting, music, climate, and more.

Morgan Thomas
Rhino Digital, LLC
+1 504-875-5036
email us here
Visit us on social media:
Facebook