Three Reasons to Upgrade Your Access Control Technology

Introduction

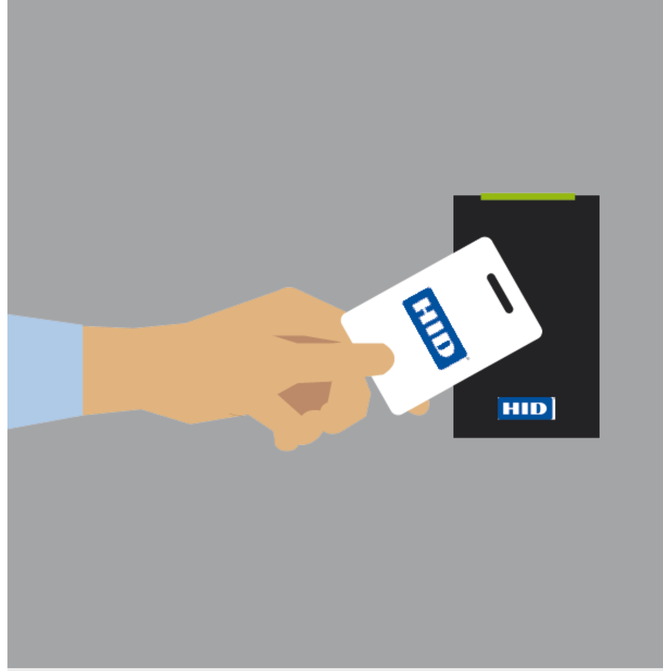
The security landscape continues to evolve in new and complex ways. This evolution brings change on many levels, which offers an opportunity for improvement rather than an interruption or a distraction. This concept has never been more important as you face today's combination of new technologies, escalating security threats and the need to **derive greater value from the access control infrastructure** while solving increasingly complex system integration challenges.

Upgrading from older, legacy technology to a new access control standard is a significant initiative. However, recent advancements have made this transition easier. Organizations can now move from solutions to more dynamic access control technologies that provide greater value. Adopting a new technology standard allows organizations to take advantage of **enhanced functionality and a higher level of security**. Access control is moving to more integrated systems with multi-layered security that can include multiple facilities. Today's more dynamic solutions allow organizations to embrace new levels of convenience and utility.

Organizations need not only support the requirements of today, but must also look ahead to the needs of tomorrow. The initial motivation to adopt a new standard of access control may be to improve security or to **consolidate multiple locations under a single standard**. Now is the time to use advances in access control to build a foundation for addressing unanticipated change and evolving security threats. Strong organizations will take full advantage of the opportunities that upgrading to a more modern solution affords.

New technology standards support a wide range of high-value applications from mobile access and cashless vending, to time and attendance, and secure print management and network login.

Three Reasons to Upgrade



1 Data privacy

As a result of new legislation or regulatory requirements, an organization may be required to increase its security. Similarly, if a company acquires a new client needing a high level of safety, there may be requirements to improve access control. New building tenants may also trigger the need for greater building or campus security, either to protect the parent organization or to comply with the tenant's requirements.

Implementing new, more dynamic access control technologies provides many benefits over maintaining older, more static ones. Organizations are facing an environment of evolving threats, and the challenges of maintaining the security and privacy of identity data are ever greater. Growing demand for a higher level of security and the convenience of using **mobile devices for access control is driving change** and spurring innovation.

The unfortunate reality is that sometimes it takes an unexpected event or security breach to prompt an organization to upgrade their access control system. By making the right steps in moving toward a more reliable, upgraded access control standard, organizations can meet the need for security and privacy with confidence, **leveraging investment well into the future**.

2 User convenience

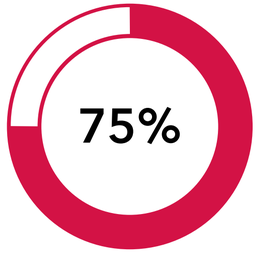
The freedom to move access control to phones, tablets, wristbands, watches and other wearables offers choice and convenience to end users, along with new and more convenient ways to open doors and gates.

Today, **smart devices are always on hand**. Users do not have to maintain and carry multiple cards or keys. In parking garages or at driveway gates, for example, the longer reach of the Bluetooth Smart communications standard makes it possible to drive up to the gate without having to roll down the car window and reach out to activate a reader.

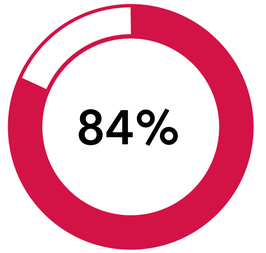
Some smart device sensors, most notably the gyroscope and accelerometer, enable **gesture detection**. This offers an additional benefit for access control: the ability to open doors from a distance by performing intuitive gestures. This provides an extra layer of authentication for added security.

It is predicted that there will be nearly 155 million smart wearable devices in use by 2019[2]. These truly "always-on" devices are even more natural candidates for access control applications because of the **ready-to-use convenience** of a wearable device.

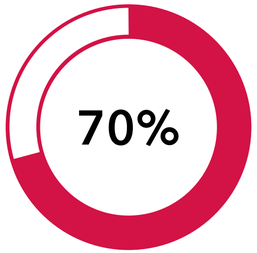
1 IFSEC Global, The Access Control Report 2016: Legacy Infrastructure and Motivations for Upgrading, 2016 (sponsored by HID Global)
2 IDC, Worldwide Quarterly Wearable Device Tracker, June 2015



75% of security professionals polled are more likely to upgrade if there is strong demand from employees for better access control[1]



84% require different levels of access depending on an individual's authority[1]



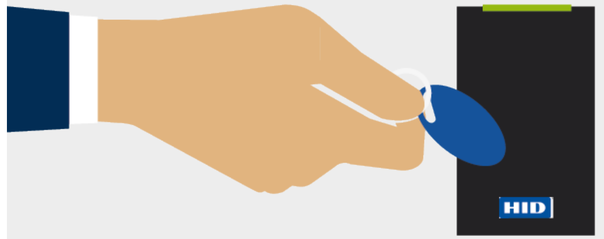
70% require access control for areas other than doors and entrances[1]

3 Flexibility

Organizations need a platform that is **flexible enough to support multiple applications** for managing not only physical access (e.g. buildings) but for managing logical access (e.g. computer/software login, time and attendance, etc.) as well.

Organizations that want to add new applications, such as time and attendance, secure print management, biometrics, cashless vending and more, will need to issue an associated card to users. This requirement can be used as an **opportunity to migrate** to a contactless wearable or smartphone that combines access control with these or other functions, enabling employees to carry a **single device for many purposes**.

Administration of these functions should be **centralized into one efficient and cost-effective system** to enable organizations to create a fully interoperable, multi-layered security solution across company networks, systems and facilities. In the future, they can migrate to the convenience, editability, and security of carrying digital keys and credentials on smartphones and other mobile devices.

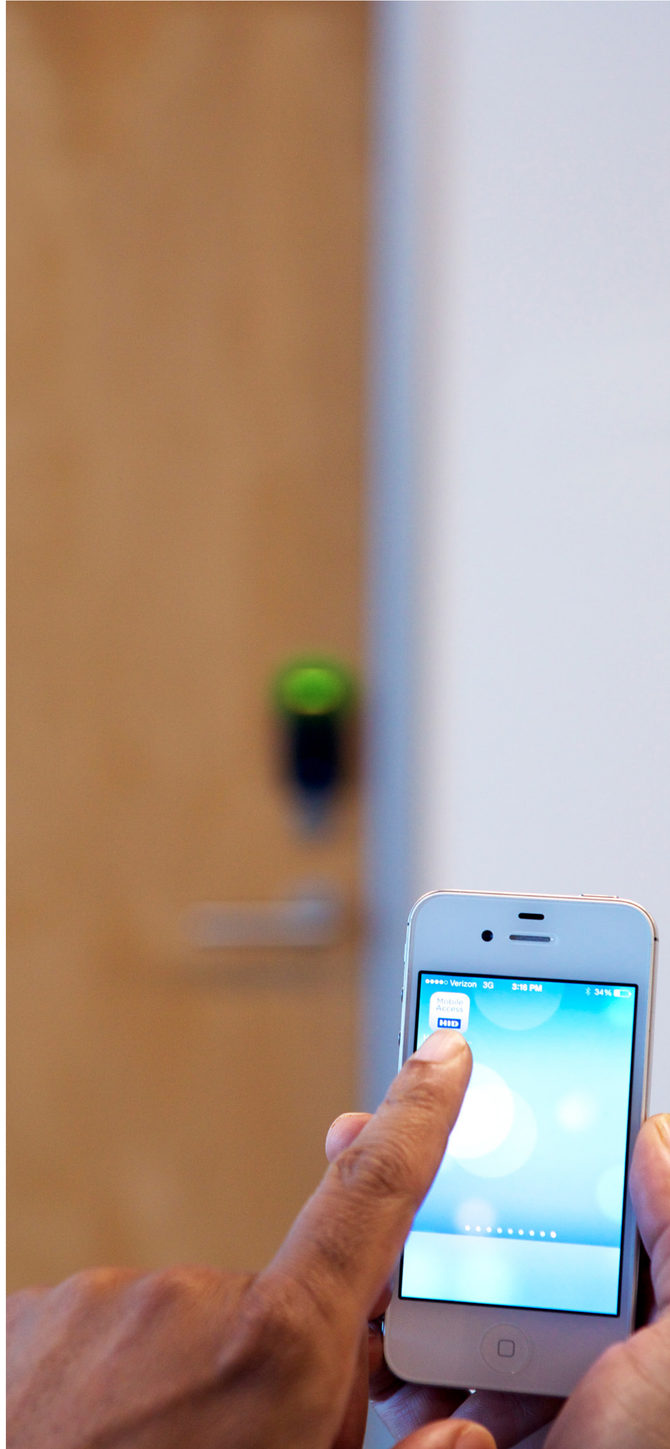


Data Privacy, User Convenience and Flexibility Go Hand in Hand

Organizations have been tasked with keeping up with a variety of technology changes that impact the physical access control (PACS) infrastructure. These changes include accommodating two-year PC refresh cycles, 18-month average mobile device lifespans and policy changes surrounding the move to “Bring Your Own Device” (BYOD). Additionally, there is **increased network access via mobile devices** due to the rapid growth of tablets, laptops and smartphones.

Legacy security solutions often use proprietary technology that is static, providing little or no possibility for functional enhancement, or the ability to offer **higher levels of data privacy**. This inability to adapt makes them easy targets for attack. Often, legacy technologies are anchored to obsolete software, devices, protocols and products, making it difficult for the access control infrastructure to facilitate change.

Built on breakthrough technologies, the latest high frequency access control systems ensure security is independent of hardware and media. This makes it much easier for organizations to support new functionality and higher levels of data privacy. They also enable the provisioning of secure identity credentials to smart devices, offering organizations the choice to use smart cards, mobile devices or both. Additionally, they offer **functionality for access control beyond the door**, which may include secure print release, network access, time and attendance or cashless vending.



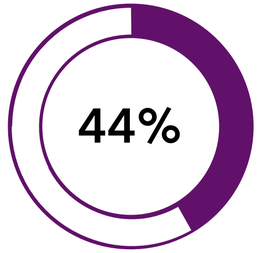
Upgrading Your Access Control Technology: A Solid Investment

If you continue to invest in outdated technology, you will never be able to progress to best-in-class access control security and data privacy management or its convenience and functionality. If you begin replacement of older systems with the new technology standards, even gradually over time, you can **minimize the risk of a serious breach** in future. The best approach is to be proactive.

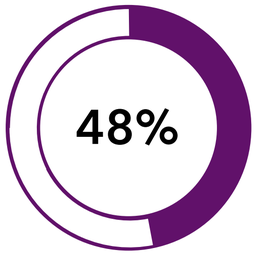
There are many reasons that organizations avoid or delay change. These include budget limitations and impact on productivity and workflow. Delaying change can be especially dangerous in the access control infrastructure, where a combination of technology obsolescence and escalating security threats can quickly cripple an organization's ability to protect its people, facilities and data assets.

Access control solutions should enable organizations to **adopt future capabilities without disrupting ongoing business operations**. While investment is required for change, there is also positive return on that budget commitment. Return on investment is realized through improved security operations, more efficient workflows and/or reduced insurance premiums due to better risk management. Taking steps to avoid a security event impacting the organization's workforce or customer data can **prevent costly long-term legal issues or brand effects** that may take years to overcome.

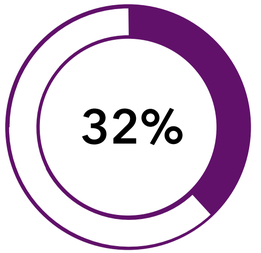
1 IFSEC Global, The Access Control Report 2016: Legacy Infrastructure and Motivations for Upgrading, 2016 (sponsored by HID Global)



44% of security professionals polled plan to upgrade their access control system[1]



48% stated 'ease of use' as the most important advantage required in a new system[1]



32% stated 'multiple levels of access depending on authority' most important in a new system[1]

Conclusion

Embracing the positive aspects of change requires an access control platform that meets today's requirements and is flexible enough to respond to future needs, all while meeting the highest levels of **data privacy, user convenience and flexibility**.

If you would like to find out how HID Global can help you upgrade your existing system, request a consultation from one of our Sales Advisors. Please send us an email and we will be in touch.

CONTACT US

Find out why HID Global is trusted by companies around the world to safeguard their facilities, assets, networks and cloud resources by visiting **hidglobal.com/access-control.**

North America: +1 512 776 9000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 5081 1650

2016-12-06-hid-global-pacs-upgrade-story-eb-en PLT-03113

An ASSA ABLOY Group brand