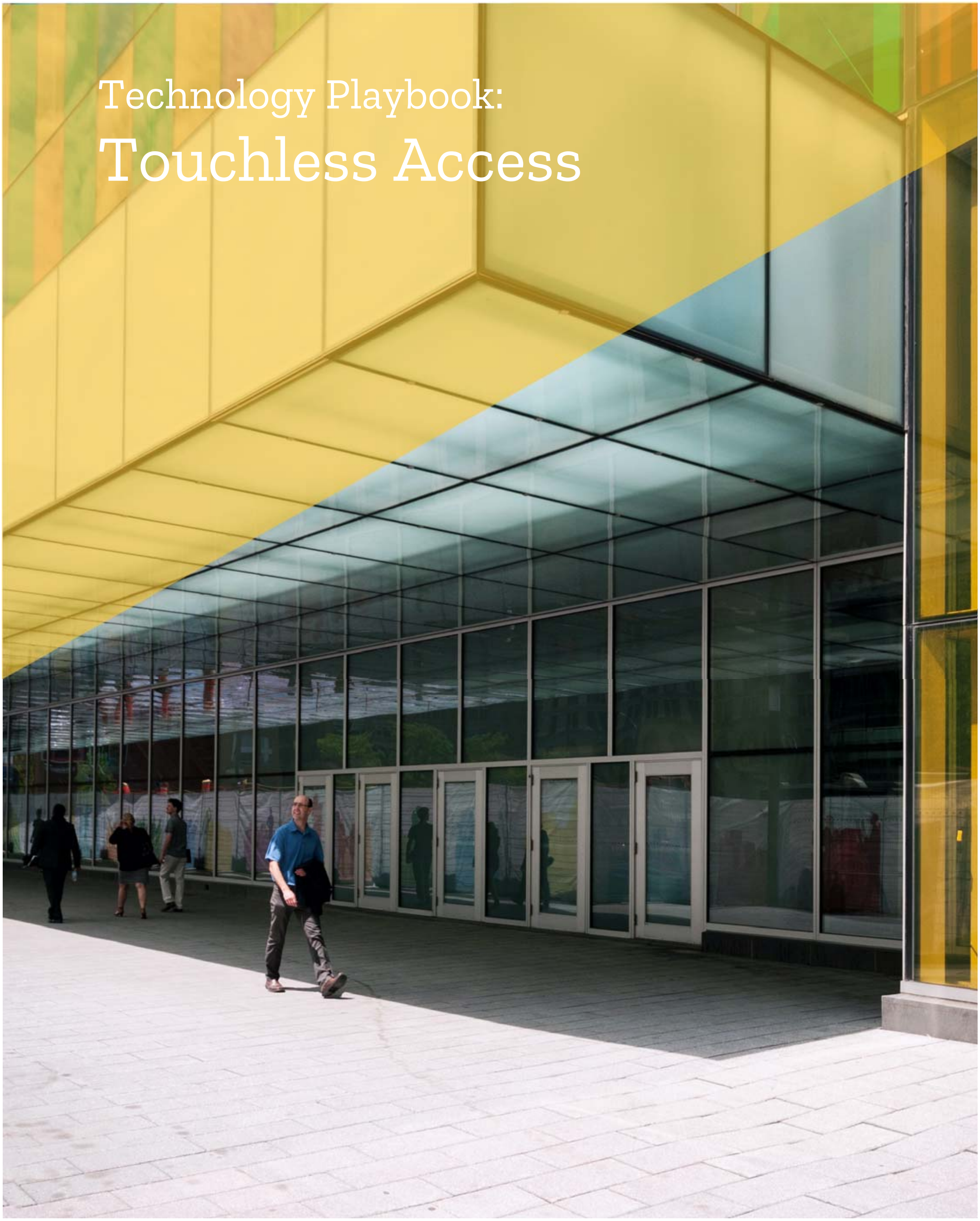

Technology Playbook: Touchless Access

For those who manage to make a difference.

INSTITUTE OF REAL ESTATE MANAGEMENT

Technology Playbook: Touchless Entry
©2020 by the Institute of Real Estate Management of the National Association of Realtors®

Disclaimer of legal liability

The Institute of Real Estate Management, including without limitation its officers, directors, employees, advisors, consultants, committee members, task force members, agents, volunteers and members ("IREM"), has assembled the material in this document for the sole and singular purpose of providing potential practices for use by those engaged in real estate management.

The information contained herein is not meant in any way to advocate, promote, or suggest any preferred method or methods for addressing the issue at hand. This publication or any part thereof does not, and is not intended to, create a standard of care for any real estate professional or property manager. This publication or any part thereof does not, and is not intended to, create any relationship of any kind whatsoever, or create any duty of care between IREM (or any of the persons or parties included in IREM as defined) and any other person or entity including any person or entity that may read, review, use or become aware of this publication or any part thereof.

The information is presented "as is." IREM makes no express or implied representations, warranties, guarantees, or promises, that the information presented is current or accurate at any point in time, be it currently, previously, or at any time in the future.

Because of changing and varying national, state/province, and local laws and regulations, competent professional advice should be sought prior to the use of this publication and any related document, form, exhibit, or the like. This publication is provided with the understanding that the publisher is not engaged in rendering legal, accounting, or any other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

By accessing, downloading and/or reading this Guide, the User expressly accepts and agrees to abide by each and every aforementioned term of this disclaimer.

Table of contents

Introduction

Providing building access systems that offer both a high degree of security as well as ease for the user have always been a priority for building owners and managers. In a pandemic environment, an additional new factor has emerged as employers in all industries seek practical guidance on how to address workplace illness and infectious disease concerns. In ensuring that they provide safe workplaces, employers are assessing all the ways they can reduce employee risk once they return to work.

This is where touchless technologies come into play. The concept of "healthy workplaces" is no longer simply about such features as open staircases to encourage movement that boosts wellness and productivity. Attention has shifted to interventions focused on reducing viral transmission risk. One of the main concerns is entry to and from work spaces, specifically where existing access systems could give rise to the possibility of spreading the virus.

In the pre-COVID-19 environment, offices were beginning to evolve to accommodate more flexible working conditions with businesses providing next-generation security with fast and reliable access control. The right solution increases worker satisfaction, reliably keeps employees safe, and effectively manages various risks. This access control needed to have an open API that could connect to modern apps, such as Slack, and other office support systems, such as guest management and video, to provide a truly user-friendly interface. An open API, sometimes referred to as a public API, is an application programming interface that is made publicly available to software developers. An API is a software intermediary that allows two applications to talk to each other. In other words, an API is the messenger that delivers your request to the provider that you're requesting it from and then delivers the response back to you. It is simply something that sends information back and forth between a website or app and a user.

These factors are still important. Now, in addition, is the sudden demand for the elimination of health risks. The health-related shortcomings associated with conventional entry access systems, complemented by continuous innovations in technology, have led to the increased adoption of keyless entry access systems and, more specifically, touchless access systems.

These systems are being driven by a number of factors:

- The outbreak of COVID-19 requires safer work environments for the users of office space. Keyless and touchless entry will be a major initiative in order to create safe working environments while also helping to reduce the spread of the virus.
- Touchless access systems reflect a sleek, modern technology that indicate the office is on the getting edge and represent an amenity that creates an enhanced end user experience sought by building occupants.
- These systems provide heightened security, keeping trespassers or visitors out of protected areas, creating peace of mind among occupants, and enabling the tracking of who enters and leaves the premises or restricted zone. Declining crime rates have been seen with the adoption of keyless entry systems.

- There is increasing affordability as declines in prices of hardware components, such as sensors, have been seen.

At the same time, there are restraints that limit the adoption of touchless entry systems. Chief among these are:

- High initial cost. Despite recent declines in cost, one of the primary factors hampering the growth and adoption of touchless entry systems continues to be the high cost associated with these products, especially biometrics, smart card, and remote access systems. Due to this, traditional security and key-dependent entry/door systems are preferred in comparison to these expensive keyless solutions.
- High replacement cost.
- Lack of infrastructural development and standardization.
- Quick obsolescence – there's a good chance what you put in today may not be used in a few years (e.g., the "Betamax fear").
- Ongoing industry consolidation.

Types of touchless access systems

Keyless entry systems are quite simply systems that provide access without the requirement of a key and are available in the following types:

- Keypad unlock systems,
- Biometric systems, which can be subcategorized into various types, such as fingerprint, facial, voice, and iris recognition,
- Card-based systems, which use smart cards, proximity cards, and magnetic stripe cards, and
- Remote access systems.

While keypad unlock systems had been gaining popularity, COVID-19 brought that to a sudden halt as attention shifted away from screen-tapping and button-pushing to touchless systems that reduce contact with potentially contaminated surfaces. For that reason, keypad systems are not being addressed here.

In addition to serving as a frontline defense to reduce virus spread, the other types of systems offer an enhanced end-user experience and respond to a heightened need for security of premises. Beyond fulfilling the primary purpose of granting access, these systems also can be used as identity management systems, together with time and attendance management systems. Also being witnessed is preference for multi-modal systems – i.e., keyless entry systems with two or more modes of access – over single-modal entry systems. Of all the types, biometric systems are the most preferred owing to their applications across a majority of industry verticals.

Biometric systems

In access control, credentials can be categorized as something you have (a key card), something you know (a PIN code), or something you are. Biometric credentials fall under that last category. They include data like fingerprints, palm veins, and retinas.

The primary types of biometric systems are:

- Facial recognition: Biometric terminals accessed via the recognition of an individual's face – in much the same way that many people now use their faces as their passwords on the newer model Apple iPhones.
- Iris recognition: Biometric terminals accessed via the recognition of an individual's iris.
- Signature recognition: Biometric terminals accessed via the recognition of an individual's signature.
- Fingerprint recognition: Biometric terminals accessed via the recognition of an individual's fingerprint, which is becoming much less appealing in light of Covid-19
- Others: Biometric terminals accessed via the recognition of any other method, such as palm, voice, ear, etc.

Biometric reader pricing ranges from low end (a fingerprint scanner) to high end (multi-input readers). A deterrent to biometric systems is that, due to personal privacy concerns, some employees may not feel comfortable using biometrics for office access. These systems also tend to be faulty in inclement weather and can be affected by dust, sand, or humidity. Fingerprint readers run the additional risk of creating hygiene issues.

Card-based systems

Whereas biometric systems provide access based on something you are, card-based systems provide access based on something you have – in this case, a key card or fob. The two main types of card-based systems are RFID cards and magnetic swipe cards.

RFID key cards and fobs tend to be popular choices for access control because they're relatively inexpensive. The underlying technology in key cards and fobs is RFID, which stands for Radio Frequency Identification. RFID key cards come in a variety of formats and protocols, with the two primary being proximity cards and contactless smart cards.

Proximity cards, which can be made of several different materials, work by being held in close proximity to the card reader without having to make contact with the reader. These cards communicate using low frequency fields (typically 125 kHz). They typically use the Wiegand protocol to communicate with the card reader and have a short read range of one to 10 centimeters and typically provide no encryption.

Contactless smart cards are more advanced. They build on and improve the technology of the proximity card and contain a smart card microchip that communicates using high frequency fields (13.56 MHz). One of the common protocols for these cards is ISO/IEC 14443-A, and the read range is one centimeter to one meter, depending on whether the credential has its own power source and size of the reader. These smart cards can provide encryption, but it is not always enabled.

Magnetic stripe or "swipe" cards are the second type of card access. They use the same technology as credit cards: a magnetic stripe stores data, which is read by a swipe card reader. The kinds of swipe cards used in access control are high-coercivity (HiCo), meaning they require more magnetic energy to encode which makes them harder to erase and therefore more secure and reliable than low-coercivity (LoCo) cards. However, swipe cards are still considered less secure than RFID cards because they're usually not encrypted and are easy to clone.

Key cards and fobs are less expensive and easier to manage than traditional metal keys but aren't always the most secure or reliable – because they're easily lost, easily cloned, or wear out quickly.

Here are a few reasons why they are far from an optimal solution:

- Easily lost or stolen. It's common for employees to forget or misplace their key cards on a regular basis. In addition, visitors can inadvertently forget to return cards, creating a security risk.

- Not always secure. Not all key cards are the same – some cards, like MIFARE DESFire EV1, are designed to prevent key cloning. Other cards that use the Wiegand protocol are more vulnerable to sniffing and copying.
- Cumbersome to use. With all the convenience RFID technology provides over traditional keys, it still requires the user to fish the key card or fob out of their pocket or handbag to present to a reader.

Remote or mobile access

Remote, or mobile, access systems are gaining interest and reflect a shift from community devices to personal devices. These are door and entry systems that are accessed remotely using a smartphone, laptop, or tablet application. This system uses mobile credentials to unlock entries. In the access control administrative software, a user is assigned a mobile credential. The user installs the access control mobile app on a smartphone, logs in, and approaches a reader. The user then makes an unlock request using that smartphone — either by tapping a button in the app, holding up the phone to the reader, or by simply touching the reader with their hand while their phone is in their pocket or bag. This request can be sent to the access control unit (ACU), also known as an access control panel, or a controller through the reader via Bluetooth low energy, via Wi-Fi, or through cellular data. Once the mobile credential is authenticated and authorized, the entry unlocks.

Privacy and security

Touchless technologies and in particular ones that use biometric data are coming under increased scrutiny on the basis of how they use and store their data. This has led to numerous states implementing strict consumer biometric data protection laws. Illinois, Texas, Washington, Louisiana, California, Oregon, Arkansas, and New York all now have biometric privacy laws in affect while a number of other states have proposed biometrics laws waiting to be passed.

Biometric data includes all the physical characteristics that can be used to digitally identify a person. These physical characteristics can include DNA, retinal scans, fingerprints, or other characteristics such as the shape of a person's hand or face or the sound of their voice. As more and more touchless technologies are implemented across the industry, it is important for property managers to be aware of the potential risks when implementing tenant-related biometric policies and procedures.

Property managers should review and revise their contracts and terms of conditions with third-party vendors to cover new biometric privacy laws and developments in the existing laws. In order to stay compliant with the evolving legal landscape it may be worth consulting with legal experts before implementing any such systems which collects personal and biometric data about tenants.

In order to maintain best practice, these guidelines should be followed:

- Ensure notice is provided to tenants that covers information relating to capturing of their biometric data; this should include the type of technology being used, the purpose for capturing the data, how the data will be captured, and how the data is being stored.
- Obtain consent from the tenant for the collection and storage of biometric data where applicable by law.
- Apply secure protocols for the storage of this biometric data.
- Insert applicable provisions in third-party vendor contracts to ensure they comply with existing laws and have the right to be notified in the event of a suspected breach of the data.
- If storing biometric data, ensure you or any third-party vendor who may be storing biometric data on your behalf, is not selling the data.

Decision factors

Selecting the right access control system can be difficult. Determining the right solution will depend on a variety of factors such as the size of your business, budget, the number of readers required, your tenants' needs, and your business objectives. When assessing touchless entry or access control systems for implementation in an office or throughout a building, there are a number of factors to consider.

Key considerations

Safety. Keyless entry has often been a nice-to-have feature in the past within the office. In the new workplace, with workers health at stake, touchless door entry may soon become a need-to-have.

Security. The number one job of an access control system is security. The hardware must be tamper-proof, software should be updated routinely to protect against potential vulnerabilities, and credentials should not be unencrypted, easily copied, or shared. Better systems enable modern security practices like multifactor authentication to ensure that administrative control stays in the right hands.

User experience. The access control system should be easy to configure for administrators, as well as convenient and simple for employees and tenants to use.

Reliability. A system should have a proven track record of server uptime and a consistent unlocking experience. Many solutions can be either unreliable or create too much friction. Best-in class-reliability calls for multiple forms of communication to authenticate an action. When Bluetooth, WiFi, and Cellular Data can be used simultaneously, the signal to unlock an entry is more reliable and the user can seamlessly enter a given space.

Flexibility. A system should allow the user to configure the convenience and security of each door or entry per user requirements. In order to meet these security requirements, it should ideally have two-factor authentication or multi-factor authentication.

Remote management. Can changes be made remotely and by the user or management, or do they need to be made on site or through a common center? Flexibility is increasingly important.

Cost. Most electronic access systems range from $1,000 to $4,000 per door installed for hardware and installation. You'll need to decide how many doors and entries you want to secure: exterior doors, interior doors, parking gates, elevators, and so on. In addition, if you are going with a cloud-based solution, you may need to pay a monthly subscription cost.

Questions to ask

These are some important questions to ask in order make sure you are getting the best system that aligns with your business needs.

How reliable is the access control system?

Electronic readers and access control systems rely on a number of different technologies which can include biometrics, Bluetooth and Wi-Fi. However in order for these systems to provide accurate readings they require continuous power and uptime. Power outages, internet outages and other miscellaneous events can cause the system failure and therefore have some sort of reliability issues.

Does the access control system integrate with existing security infrastructure?

In most scenarios, buildings already have some sort of security in place with video surveillance and alarm systems to create safe work environment and protect the building. Recent advancements in video management systems allow for number plate recognition, head count and even predict certain events before they happen. It is important to ensure that your access control system can integrate with your VMS to create greater efficiencies.

How does your system work with intrusion detection?

Intrusion detection technology is a newer feature on most access control systems. This feature allows companies to lock or unlock doors all at the same time by using some type of authenticated device such as a card or fob. This feature also eliminates the requirement of having someone lock every door upon departure.

Can this system integrate with existing office automation functions?

Businesses can add enhanced functions to their access control system such as visitor management, lighting and room booking to help provide a more automated office.

Will employees be able to easily use this system?

Additional technology for employees can sometimes cause friction. For example the extra steps involved in unlocking ones phone or having to line up your eye directly into a biometric reader can cause delay and with that some frustration. Some users prefer more simple methods such as key cards which only require a quick swipe.

How will a modern access control solution evolve with my business?

In order to be as flexible with new applications and future technologies, businesses should invest in access control systems that are based in the cloud and have open APIs.

Does the system support occupancy management needs?

With the need for social distancing brought on by COVID-19, occupancy management has become critical, and with it the ability track people who enter and exit a building and control the number of people in a given space at any time.

What security features does the access control system have?

Cloning and lost or stolen access cards are common problems for any access control system and can have a major impact on the integrity of the company's security. The use of multi-factor authentication to provide tenants with an added layer of protection to ensure that the correct user is gaining access to the correct areas of the building. Time-based entry is another security feature enabled by cloud-based access control. Finally, the system should have a back-end system that enables real-time monitoring to determine each irregular entry, ajar notifications, and any failed entries that take place.

How does your solution work with controlling elevator and garage access?

Buildings are starting to deploy access control systems in elevators and garages to help create a more secure environment. Smart elevators, which allow passengers to request a particular floor before getting on, are becoming more common but can require access cards to operate. Garages may have existing security barriers in place.

Can your system handle inclement weather?

Cold weather, heavy rain, or thunderstorms can make readers malfunction. If a system reader is being installed outside, you should look to see that it has at least an IP65 rating.

What sort of mustering scenarios does the system handle?

Mustering is one of the most powerful tools in an access control system. It allows administrators of the system to use access logs to locate people in a building or specific area. It can not only help with time and attendance tracking but also use time logging to track a user's movement throughout the building and provide insights into where a user was at a given time. This can be very helpful when it is necessary to track potential criminal activity.

How will compliance be addressed?

Meeting a business's compliance needs is one of the biggest considerations in choosing access control systems. These are some of the requirements that building managers may be asked to meet:

PCI Security Standards Council. Requirements 9 and 10 are common areas to address in physical and network security. Requirement 9 mandates organizations to restrict physical access to a building for onsite personnel, visitors and media. The business should have adequate controls to ensure that no malicious individuals can steal sensitive data. Requirement 10 relates to the need to track and monitor systems.

Health Insurance Portability and Accountability Act (HIPPA). Although most think of this requirement within the healthcare context, employers also deal with a large amount of health information. For instance, when an employee requests medical leave, employers need to keep any documentation of that absence confidential. In order to meet this requirement, businesses can use access control to keep this information locked in a storage room.

SOC 2. - SOC 2 compliance is a component of the American Institute of CPAs (AICPA)'s Service Organization Control reporting platform. This auditing procedure enforces service providers to manage data to protect employee and client privacy. Companies in the SaaS space are eligible to receive SOC 2 certification by purchasing an access control system with two-factor authentication and data encryption. Any business dealing with customer data must protect PII (personally identifiable information) from unauthorized access.

ISO 27001. The requirements of the ISO 27001 standard expect monitoring, measurement, analysis, and evaluation of the Information Security Management System.

This information security standard requires that management systematically examines an organization's security risks and audits all threats and vulnerabilities. It also requires a comprehensive set of risk avoidance or transfer protocols and have an overarching management process to ensure that information security continues to meet the business's needs on an ongoing basis.

CJIS. In 1992, the FBI created this organization to monitor criminal activities through analytics and statistics. Today, the organization has a few best practices related to security and authentication. From an access control perspective, this includes restricting access based on physical location or time of day.

Assessing the company

With real estate still being a somewhat nascent technology sector, there are many new companies offering their products. Here are some key questions to ask when evaluating a product or service from a new company – most of which can be answered by conducting a simple search on Google, Crunchbase, or TechCrunch.

How long has the company been in business?

Is the company a startup? If it is a startup, what type of funding is backing it? When looking into a company that you are thinking of using, you want to be sure that the company will be around in the coming years. One good indicator is looking at the financial backing it has received from reputable investors. It is generally positive if a notable venture capital team has backed the company (e.g. Fifth Wall, JLL Spark) or it has received sufficient funding that will allow the company to grow in the coming years.

What is known about the company's ownership and management?

Is it a private company or public company? Who are the people behind the company? What is their background, their reputation, their past experience and performance? Is there a capable management team in place? Do they have the technical capabilities to make the company work?

Does the company have a webpage?

Does the webpage present complete information about the company and its management team as well as the solutions it offers? Does it provide sufficient technical details to indicate the product is beyond the conceptual stage?

What is the company’s standing and track record?

Who else is using the company’s product? Do other credible users recommend the company and its solution? What are the security protocols and standards for the company?

What would an exit strategy look like?

If you choose to abandon the company in the future or it goes out of business, what barriers would exist? How easy would it be to migrate your data to another platform?

Touchless access system providers

What follows is a listing of several providers of touchless access systems. Others are also available in the marketplace.

A note about pricing: This playbook aims to give a snapshot of some of the leading providers of this technology and service in the marketplace today. As each technology provider has different pricing models and each property manager has different requirements, functions, number of users, and needs, providing specific pricing information is problematic. You are advised to contact the provider directly in order to get the most accurate price plan that caters to the specific needs of your company and your properties.

- ASSA ABLOY AB
- Aware
- Anviz Global
- Daon
- Datawatch
- Idemia
- Kastle Systems
- NEC
- Suprema

ASSA ABLOY

ASSA ABLOY AB is building material manufacturing company that specializes in offering door opening solutions. The company offers its solutions across hospitals, residents, hotels, educational institutes, corporate offices, etc.

The company, due to its wide product portfolio of keyless access systems and its subsidiaries offering the same solution, is a major player in the market. For instance, a majority of the products offered by Yale, one of its subsidiaries, cater to the keyless entry system market. The company has its operating offices in approximately 70 countries globally.

Key features of the biometric entry systems offered by the company include multiple locking/unlocking options besides biometrics as well, such as keypad lock, RFID card and remote accessibility, touchscreen display, robust design, compatibility with various types of locks, high operating temperature, etc.

AWARE

Aware is a leading global provider of biometrics software products and solutions used to collect, manage, process, and match biometric images and data for identification and authentication.

Products include complete biometric software solutions along with modular components used to build them: SDKs and applications for enrollment; fingerprint, face, iris, and voice matching algorithms; mobile biometric capture and authentication software; a biometric workflow and middleware platform, and a fully-scalable ABIS.

Anviz Global is a leading provider of converged intelligent security solutions, Anviz Global is committed to providing comprehensive IP Biometrics access control, time attendance solutions, IP video surveillance solutions to SMB and enterprises based on cloud, IoT and AI technologies.

Access control is available in these forms:

- Biometrics/readers
- Cards, card access, card readers
- Finger print
- RFID devices and readers

Daon's IdentityX® Platform, an omni-channel approach to biometric authentication, allows users to mix and match security factors of the past (e.g., passwords and tokens) with security factors of today (e.g., voice, fingerprint, facial, behavioral biometrics) as well as emerging factors of tomorrow. All these factors can be used individually or fused together to deliver the level of assurance desired.

Datawatch Systems has a long-standing record of success in managing access control for government agencies, multinational corporations or single-office suites. Datawatch Systems now offers a new product called Datawatch Mobile Access, which allows authorized users to use their mobile phones, rather than a separate access card, to access a building space, even access elevators, lighting and climate controls.

IDEMIA has developed cutting-edge technologies and services leveraging artificial intelligence, biometrics and cryptography. IDEMIA is a major technological player in the fields of identity management and authentication or security of payments.

Kastle Systems is a leading provider of cloud-based managed access control systems that has provided managed access control for commercial and multifamily spaces for more than 40 years. Kastle operates and manages security systems for its clients remotely, around-the-clock, and protects over 10,000 locations nationwide and internationally. It recently launched a new product, KastleSafeSpaces, a new system that integrates touchless access control, virus-screening and contact tracing processes to confidently facilitate a safe return to office.

NEC combines its advanced technologies, services, and knowledge and its more than 117 years of expertise as an ICT leader to help ensure the safety, security, efficiency, and equality of society.

NEC offers:

- Face recognition
- Iris recognition
- Fingerprint and palm print recognition
- Finger vein recognition
- Voice recognition
- Ear acoustic authentication

suprema

Suprema is a leading global provider of access control, time and attendance, and biometrics solutions. Operating a commercial office facility means ensuring the necessary safety, controlling processes optimally and offering the highest possible level of convenience coupled with maximum efficiency.

Suprema BioStar 2 provides a comprehensive range of secure, reliable and convenient access control features to a modern office environment. From smaller offices to multi-site corporations, Suprema delivers bespoke access control security solutions to meet dynamic needs from system integrators, installers, and end-users.

Low-tech alternatives

Part of the challenge with installing any new hardware is the approval required from a web of stakeholders, including building owners, tenants, and others who work in the space. In the case of older buildings, such installations may be especially difficult as well as expensive. And even with sophisticated biometric access systems or card readers, often the door itself must be opened by using the handle – making it anything but touchless.

These are just a few of the situations that require exploration of low-tech alternatives, at least for the short term. With health and viral transmission being a chief concern, here are a few low-tech solutions:

- Foot-operated door handles that allow a door to be opened hands-free. Simply clip the device onto the bottom of the door - then, just step on it.
- No-touch stylus door openers shaped like keys that can be used to open doors, push elevator buttons, and flush the toilet
- Providing disposal gloves to use in entering the building and the workspace – with a designated PPE disposal station once inside as well as outside the building.
- Hand sanitizer stations on both sides of all doors.

Acknowledgments

Technology Playbook: Touchless Access was developed by James Scott, IREM's Technology Innovator-in-Residence from the MIT Real Estate Innovation Lab, under the guidance of the 2020 IREM Technology Advisory Board:

Greg Cichy, CPM®, Chair
Colliers, AMO®, Arlington, VA

Paul Gottsegen, CPM®, Vice Chair
New York, NY

Kim Bender, CPM®
Fairfield Residential Company, LLC, AMO®, San Diego, CA

Edward Brownfield, CPM®
SJG Properties, Washington, DC

James Scott
MIT Real Estate Innovation Lab, Cambridge, MA

Kasara Smith, CPM®
Cushman & Wakefield, AMO®, Washington, DC

Austin Widman, CPM®
Retail Property Management, Prospect, KY

Cover photo
Photo by Scott Webb on Unsplash

About IREM®

For over 85 years, our members have made us the world's strongest voice for all things real estate management. Almost 20,000 leaders in commercial and residential management call this home for education, support and networking. Our CPM®, ARM®, ACoM, and AMO® certifications are internationally recognized symbols of ethical leadership and a well-managed property. And our tools deliver decades of on-the-job know-how to help members get even better at what they do. Put simply – IREM and its members are here to elevate the profession. If you know real estate management, come get to know us.

Institute of Real Estate Management
430 North Michigan Avenue
Chicago, Illinois 60611 USA
irem.org