THE 2020 STATE OF PHYSICAL ACCESS CONTROL REPORT

Based on research conducted by:

HID

SECURITY MANAGEMENT

KEY FINDINGS

- **March to Mobile:** Use and planned use of mobile devices as credentialing tools is increasing, which is seen as the single most impactful technology shaping access control.
- **Aging Infrastructure:** Access control infrastructure is aging, and most systems are three or more years old, yet most organizations have either no plans to upgrade obsolete systems, or plans are more than a year in the future.
- **Security Needs Are Not Being Met:** Security professionals do not have confidence that their current physical access control systems are sufficient to secure facilities or the people, data, and intellectual property they are intended to protect.
- **Physical and IT Security Collaboration:** The departments often work together on the development of security best practices and shared decision making on new technologies.
- **Opportunities for Improved Security:** Security directors have ample opportunities to positively impact security posture, user convenience, and operational efficiency by leveraging relationships with IT and prioritizing access control upgrade plans.

Security is Struggling to Keep Up with Threats, but Moving in the Right Direction

From protecting the perimeter to securing high-value assets, access control systems are a fundamental responsibility for organizational security departments. A new study of security directors, managers, and consultants finds access control infrastructure is deteriorating, as is the confidence that the access control systems in place are up for the job.

These findings come from a survey of ASIS International members and customers on access control technology; its use, important trends, and upgrade planning. A project of *Security Management* Research and HID Global, the survey was conducted in 2019, building on a similar survey completed in 2017.

The survey underscores the complexities of managing physical security at a time when increasing technological sophistication of bad actors and the potential costs of security vulnerabilities are rapidly increasing. Comparing 2019 to 2017 indicates that companies are slowly making investments in more advanced and secure access control technology, and collaboration with IT continues to be important. Mobile access continues to be of particular interest as respondents indicated increases in current and planned use of mobile access technologies. In addition to the continued increase in adoption rates, physical security directors note that mobile access and mobile apps would improve current access control systems and are shaping the future of the industry.

Industry Pulse—Trends in 2020

Access control solutions must accommodate complex interactions between an organization's business needs and its risk profiles. The procedures, protocols, and technology that comprise an access control solution must fit together seamlessly. The solution touches every employee, contractor, and visitor, so it is not surprising that on a year-to-year basis, access control solutions may not change much in any given organization. However, business needs and risk profiles change, technology advances—and while the pace may be slow—there is a trend of organizations employing technology that is more secure and easier to deploy and use.

Access Control Systems Are Aging

The survey shows that at most organizations, the basic components of access management systems are aging. The credentialing component is three or more years old at 58 percent of companies. More than 60 percent of organizations also rely on controllers and readers that

A new study of security directors, managers, and consultants finds access control infrastructure is deteriorating, as is the confidence that the access control systems in place are up for the job.

are three or more years old. The software supporting the systems is also aging: 49 percent of security directors report access control software that has been in use for three or more years. However, upgrading in the near term isn't a priority for many.

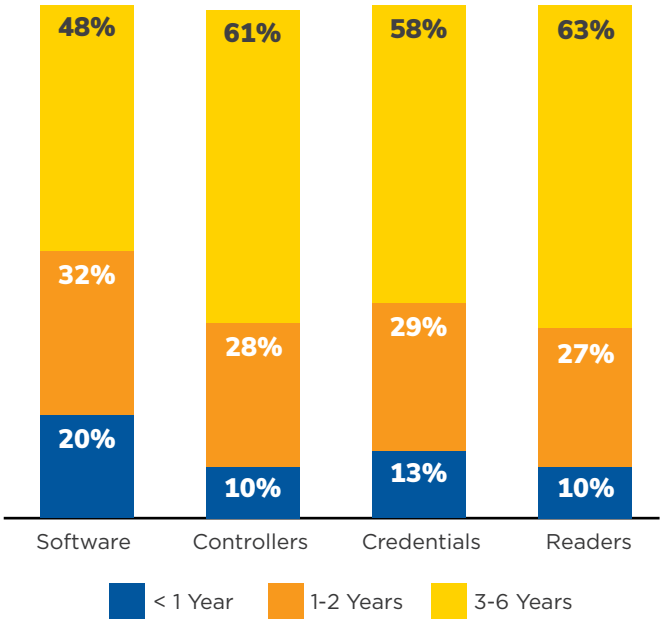
"We hear from security professionals that even though parts of their organization's access control infrastructure are several product generations out-of-date, upgrading to a robust modern standard wasn't a corporate priority," Luc Merredew, Product Marketing Director, Physical Access Ccontrol, Americas at HID Global. "However with recent highly publicized IT compromises linked to physical access, they aren't waiting any longer."

The survey presented a list of electronic access control credential technologies and asked security directors to select all the ones they employ at their organizations. Fifty-one percent report using 125 kHz low frequency proximity cards. These cards rely on radio frequency signals, technology that is 25 years old and has significant security vulnerabilities. Even older and less secure technology is also still utilized with 26 percent reporting the use of magnetic stripe cards and 17 percent reporting the use of barcodes.

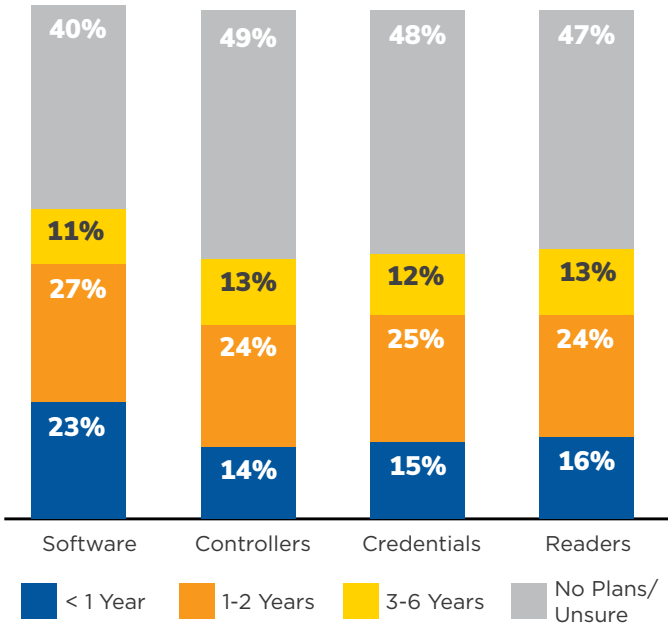
Though the technology is more than 15 years old, iCLASS cards, with their encryption capability, make a good demarcation line between technology that is more secure and technology that is less secure. These cards are in use by 45 percent of organizations. The survey also asked about several technologies that are more secure than iCLASS cards, all of which are in use by approximately one in five organizations: MIFARE Classic (21 percent), MIFARE DESFire (18 percent), FIPS-201 Standard (18 percent), and Seos (17 percent).

Overall, 54 percent of organizations use at least one of the more secure technologies. It should be noted that security departments in general have several different access control technologies in use at the same time. For example, of the respondents who

CURRENT AGE OF ACCESS CONTROL COMPONENTS

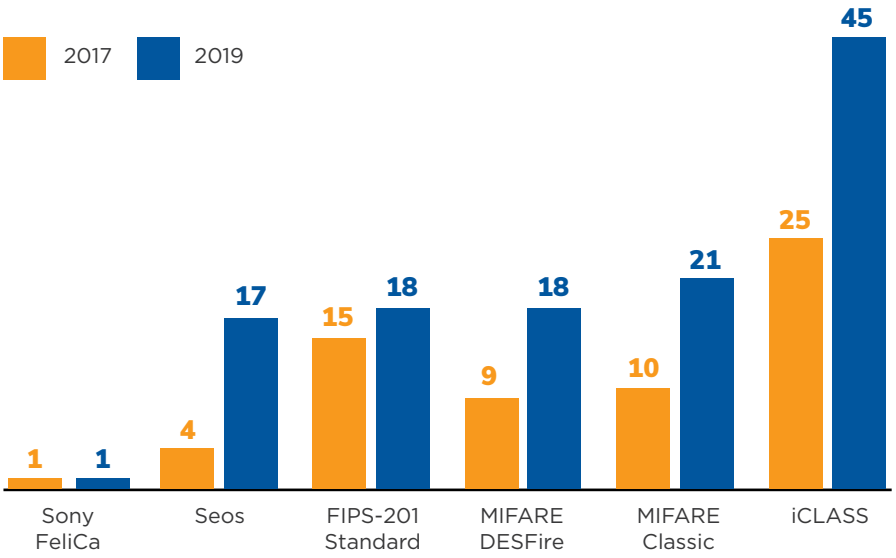


UPGRADE PLANS FOR ACCESS CONTROL COMPONENTS

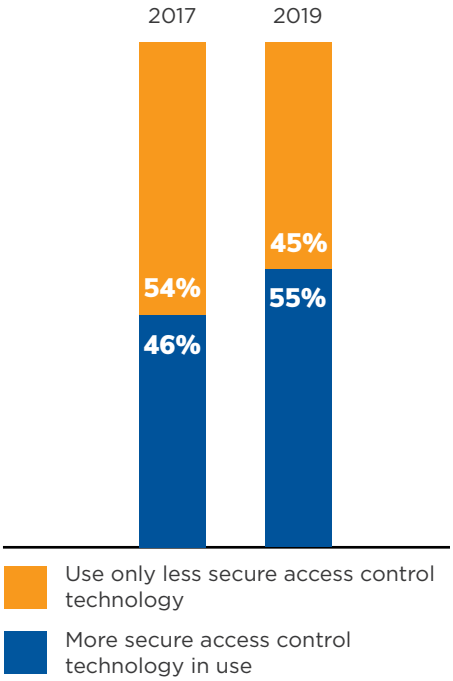


> *As migrations to more secure credentials occur, a primary goal for physical security professionals should be ensuring that options to expand and adapt to future needs are not limited.*

MORE SECURE CREDENTIAL TECHNOLOGY USE



OVERALL USE OF MORE SECURE CREDENTIAL TECHNOLOGY



reported using 125 kHz prox cards, 22 percent report also using Seos, one of the most advanced credential technologies available.

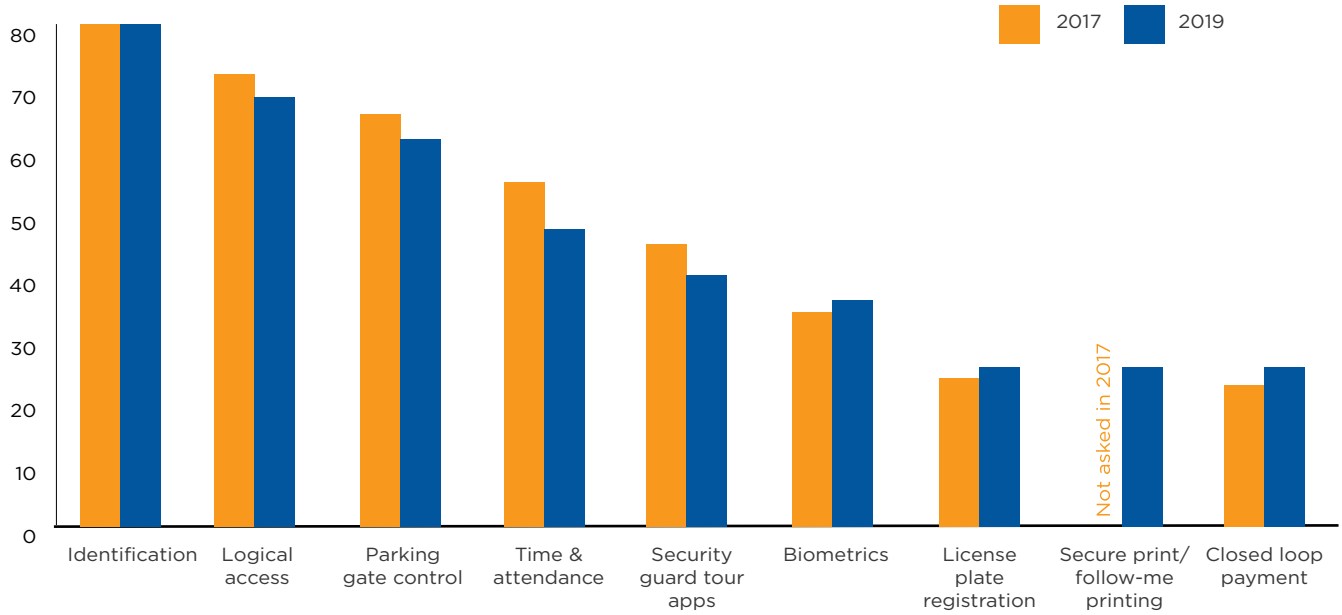
"Many companies rely on access control technology that is old— 20+ years—and is easy to clone," says Merredew. "Copying takes seconds and in many cases copies can be made at your local convenience store. As migrations to more secure credentials occur, a primary goal for physical security professionals should be ensuring that options to expand and adapt to future needs are not limited. Creating an upgrade path to mobile access that doesn't lock the organization into specific devices and communication protocols is key."

Improving Effectiveness of Systems Is Top of Mind – Especially Through Mobile

The types of access control applications used remained remarkably steady from 2017 to 2019. The most common applications are identification, including photo badges, (80 percent in both 2019 and 2017); logical access to IT resources (68 percent in 2019, 71 percent in 2017); and parking or gate control (61 percent in 2019, 63 percent in 2017). Less frequently used applications included closed loop payment (27 percent in 2019, 24 percent in 2017) and license plate registration (27 percent in 2019, 25 percent in 2017).

Use of at least one secure credential technology rose by 9 percent over the 2017 survey with use of mobile technology in access control systems indicated as another area that receives intense interest. The technology solutions promise speed, convenience, advanced security (such as built-in biometric screening on the device itself), and flexibility. Staff, contractors, and visitors will typically have a smart device with them. Activating and deactivating a credential can happen in real-time, over the air.

APPLICATIONS USED WITHIN PHYSICAL ACCESS CONTROL SYSTEMS

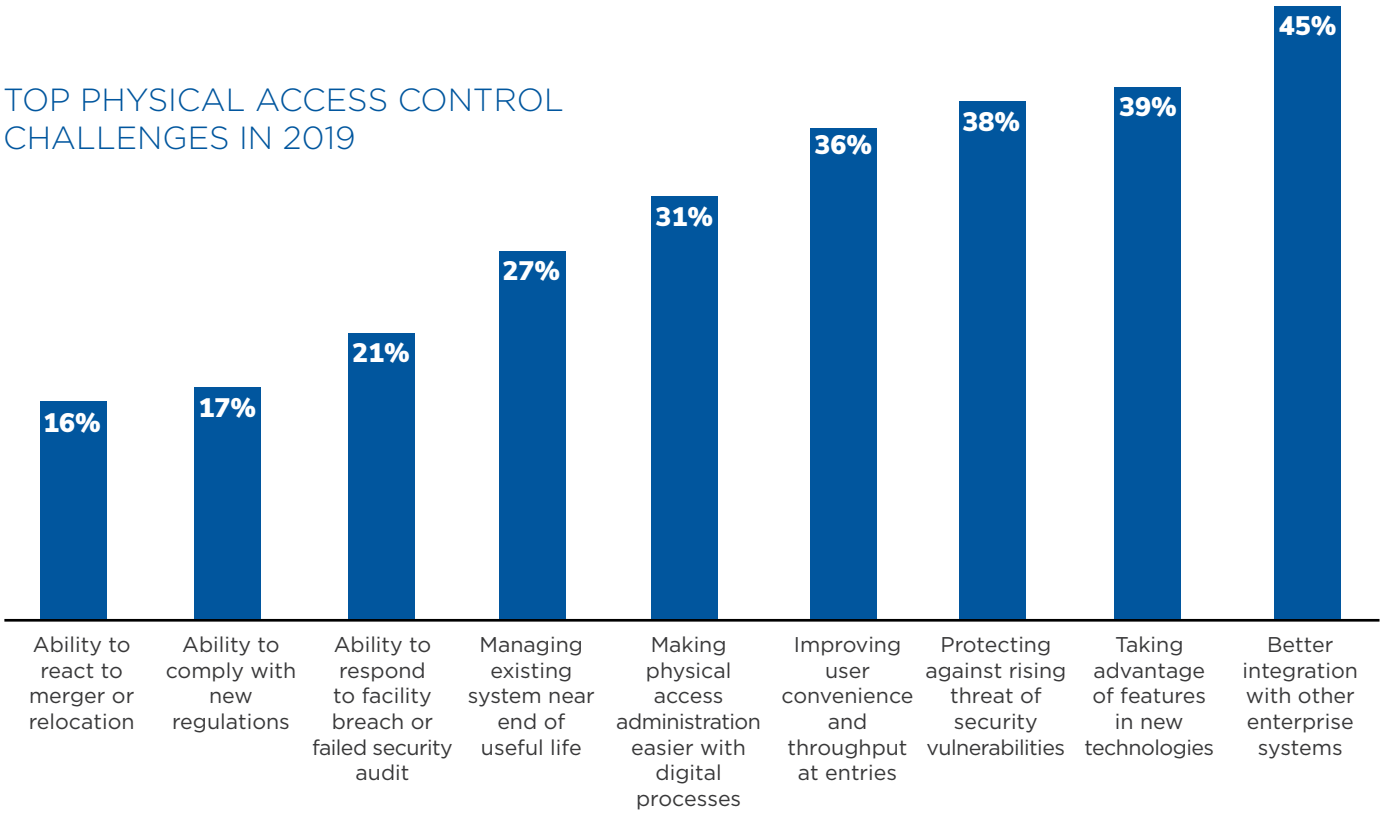


Security directors cite use of mobile access or mobile apps as the top trend shaping the access control industry in the near future (57 percent). Adoption continues to rise with 25 percent being fully deployed, partially deployed or in the process of deploying a mobile solution. Another six percent will deploy mobile-enabled readers within the next year.

Facing Challenges in 2020

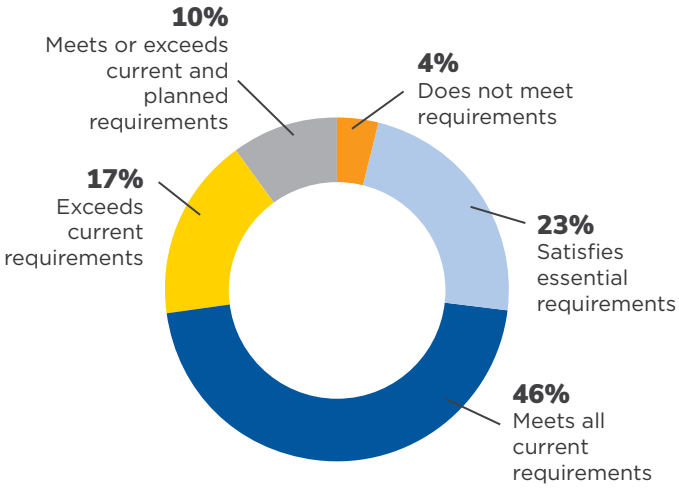
The trends uncovered in the Physical Access Control Survey dovetail with the challenges security directors describe. Aging technology and an expanding and diversifying threat environment are underscored by a desire to capitalize on new capabilities to keep people and resources safe.

TOP PHYSICAL ACCESS CONTROL CHALLENGES IN 2019

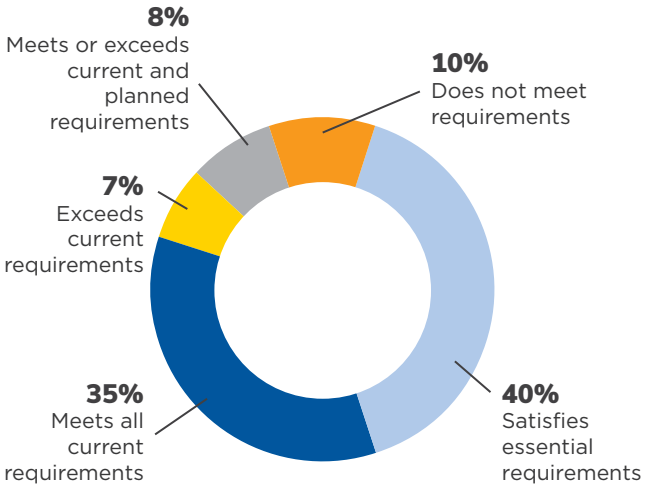


In 2017, 73 percent of respondents reported that their current solution met or exceeded all current requirements. In 2019, the number falls to 50 percent.

2017 ADEQUACY OF CURRENT PHYSICAL ACCESS CONTROL SYSTEM



2019 ADEQUACY OF CURRENT PHYSICAL ACCESS CONTROL SYSTEM



Technology Limitations Make Day-to-Day Security Demanding

Security directors were asked to choose their top three daily access control challenges from a list of nine. Issues related to technology topped the list. At 45 percent, security directors cited "better integrating with other enterprise systems" more than any other challenge. Data from access control systems has emerged as a valuable tool in business analysis and, conversely, data from other systems can be combined with access controls to mitigate risk, optimize processes, and make better safety and security decisions.

Along with integration, 39 percent of security directors see "taking advantage of features in new technologies" as a significant challenge. Employing mobile devices in access control systems, as already addressed, is one primary feature that security directors see as a step forward. More sophisticated, harder to fake credential and reader systems that leverage biometrics or enhanced encryption, are another example. Other new applications, such as real-time location services, show great promise.

The survey also highlighted the increased complexity of the issues security must deal with: 38 percent cited "protecting against rising threat of security vulnerabilities" as a main challenge. Increased incidence, severity, and publicity of mass violence have changed the way many security directors think about access control. As the methods and sophistication of bad actors continues to evolve, security directors find themselves under increased pressure and scrutiny.

To put context around how integrated systems are today, the survey asked security directors to select all the ways their organization secures access to network applications. Use of username and passwords, at almost 90 percent, is fairly ubiquitous as expected. Additional or other methods employed include: digital certificates (28 percent), tokens (21 percent), and smart cards (20 percent). Biometrics, SMS, and push notifications are used by fewer than 15 percent of organizations.

One result of the aging security infrastructure is increasing doubt about whether physical access control solutions in use today are up to the task. In the 2017 survey, 73 percent of respondents reported that their current solution met or exceeded all current requirements. In 2019, the number falls to 50 percent. Some of that is likely due to one more year of age on the infrastructure. However, the number, complexity, and

severity of the threats that face organizations also continue to increase.

Upgrading is on the Roadmap, but Mostly Remains a Future Investment

Despite an aging infrastructure, upgrade plans remain more than a year into the future for most companies. A full 40 percent of security directors report that either there are no upgrade plans for any of the components or they do not know if there are any plans.

The biggest obstacle to upgrading is budget, with 45 percent citing it as the main barrier preventing or delaying upgrades. One in five say physical access system upgrades are not a priority for their organizations, while others listed business disruption, resistance to change, and integration with legacy systems as the biggest obstacle (each of these barriers were the top reason for approximately 10 percent of respondents).

Opportunities

Security directors report the two most important ways an access control system aids an organization's security is by limiting physical security breaches (34 percent) and limiting the incidence and impact of insider threats (28 percent). To accomplish these goals, as well as realizing the other benefits of a high-functioning access control system, organizations are working to build synergies between security and IT and add functionality to their systems.

IT Collaboration and Budget Sharing

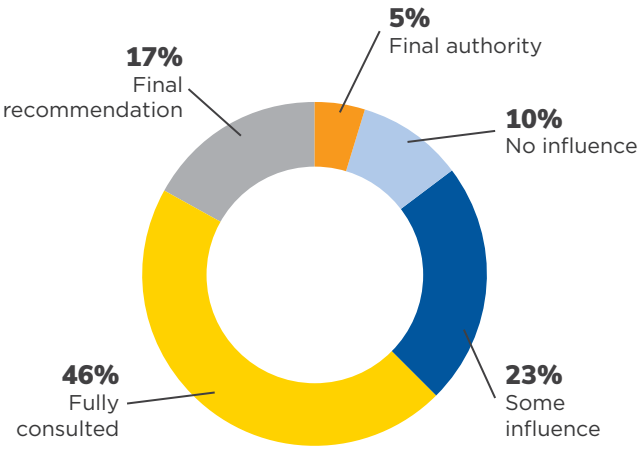
The physical security trends survey examined several different facets of the relationship between physical security and information technology and related convergence issues. Most security directors report that they work with IT departments to establish security best practices for their facilities (61 percent) and to look for new technologies cooperatively (55 percent). However, 20 percent report that there is little or no overlap between physical security and IT.

Budget status is one signal of convergence. In the physical security trends survey, 14 percent report that physical security and IT share a budget, which points to organizations where the two functions have converged. However, it would not be unusual for physical security and IT to maintain separate budgets even in converged organizations. The trends survey asked respondents to rate the level of authority on decisions to upgrade physical access control solutions: 46 percent said IT was fully consulted and another 22 percent said IT was involved in either the final recommendation or the final decision. Ten percent said IT had no influence.

Despite indicating an overall need for better integration, when asked about the concerns they have about merged physical access and logical access control systems, 50 percent of security directors pointed to difficulties implementing or prioritizing new technologies, 43 percent cited increased technological complexity, and 36 percent said it was difficult to manage multiple credentialing systems. Despite the difficulties, at 28 percent of respondents, "integrated physical and logical access control" was selected as the top technology advancement that would have the most impact on improving the organization's overall access control system.

"Today's organizations must treat physical security with the same focus and diligence exercised on IT networks," says Merredew. "Organizations recognize this and are evolving to meet this need. One way is by allocating a small fraction of the IT budget for comprehensive physical security upgrades such as addressing weak links in older physical access control systems or synchronizing audits, reviews, and upgrades."

INFLUENCE I.T. HAS ON UPGRADING PHYSICAL ACCESS CONTROL SOLUTIONS



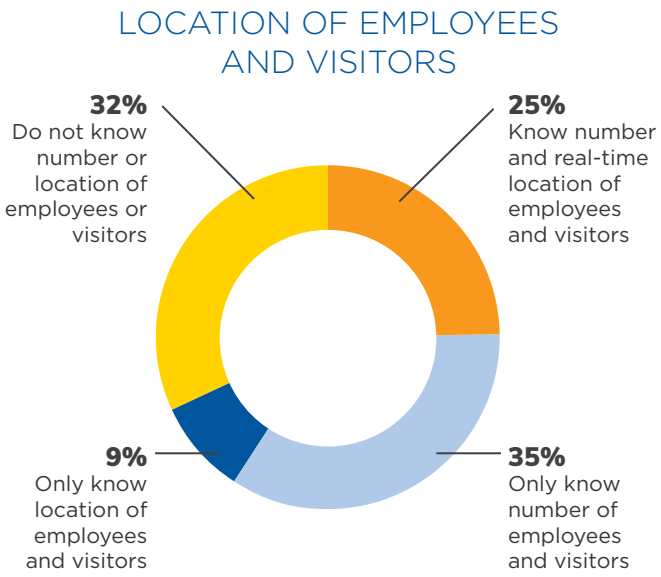
One-third of respondents reported that they do not know the number or location of employees or visitors at their facility or facilities.

Decision Making Driven by Connected Experiences

During any critical security event, such as an outburst of workplace violence or a weather-related catastrophe, the number one priority for security professionals is the safety and security of the people in the impacted area.

Of those who monitor employee and visitor location in some way, most use badge scanning as the primary tracking method: 70 percent use badge scanning for employees and 47 percent use it for visitors. A paper roster is also used with some frequency for visitors (28 percent) while time and attendance systems (21 percent) are also used to monitor employees. Using an SMS or cell phone system is not in widespread use, with only two percent reporting use of such systems for employees or visitors.

"Commercial real estate building owners and management professionals want to know what's happening in real-time in the properties they manage to improve the user experience for both the tenant and the owner," says Taylor Breihan, Global Business Development Manager, Location Services at HID Global. "Organizations have policies in place, but how effective are those policies? When the entire building is evacuating during an alarm, access control is ineffective for locating employees or visitors left inside."



This is an area of security management that is evolving along with the availability and accessibility of Real-Time Location Services (RTLS). Knowing the number and locations of all people in a facility during an emergency can be invaluable for safeguarding people and property. These systems have typically used RFID, though Wi-Fi and Bluetooth are also used, to identify and monitor the exact location of valuable assets at any given time. RTLS complements access control technology and provides data that optimizes space utilization, protects restricted areas, provides visitor and asset location awareness, and can inform use of HVAC and lighting, all of which creates a more efficient and secure workplace.

Better Security, User Convenience and Operational Efficiency

Ultimately, the industry is experiencing a trend toward adopting use of access control technologies that are more modern and secure. In 2017, only 45 percent of organizations used at least one of the more secure credentialing technologies compared to 54 percent in 2019. The rise in using mobile credentials is another sign that organizations are working to modernize their access control systems.

Much work remains, however. The importance of securing physical access to facilities has never been greater. Migrating to up-to-date physical access control systems reduces risk by removing vulnerabilities, adding multi-application capabilities, and paving the way for user-friendly credential adoption such as mobile access. And as access control technology continues to advance, forward-looking organizations can not only dramatically enhance their capability to protect their people and property, they can use access control data to improve business operations.

Methodology

This report is based on 473 responses to the 2019 Access Control Systems Trends Survey conducted by Security Management Research and HID Global. A link to the 25-question survey was emailed to more than 50,000 ASIS members and customers in the summer of 2019 and promoted through ASIS newsletters and other means. Respondent demographics, including company size, industry, and title match other recent *Security Management* Research projects, indicating a good representative sample. At the 95 percent confidence level, the margin of error for the survey is approximately +/- 4.5%.

About HID Global

HID Global powers the trusted identities of the world's people, places and things. Our trusted identity solutions give people convenient access to physical and digital places and connect things that can be identified, verified and tracked digitally. Millions of people around the world use HID products and services, and over 2 billion things are connected through HID technology.

About Security Management

As the flagship publication of ASIS International, Security Management is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

2020-02-25 hid-pacs-2020-state-of-physical-access-control-wp-en PLT-04966