The 2021 State of Physical Access Control Report

KEY FINDINGS

- **Industry Responds to the New Normal:** Security professionals report overall pandemic response, including touchless solutions, as the key driver to upgrading physical access systems.
- **Investing in Mobile:** Over half of the companies surveyed are in the process of upgrading to mobile access or have plans to deploy mobile access in the near future. This follows last year's trend predicting mobile as the single most impactful technology-shaping access control.
- **Relying on Aging Technology in the Short-Term:** While companies are marching toward mobile, they are relying on aged access control infrastructure along the way. Most companies still leverage solutions that have vulnerabilities, are inefficient to manage, or don't integrate with other technology.
- **Recognizing Opportunities:** Security professionals have new opportunities to demonstrate how upgrading access control infrastructure to respond to threats nets positive ROI while improving security, user convenience, and organizational efficiency.

REPORT OVERVIEW

The fundamental responsibilities for organizational security departments were disrupted by moves to remote working and new regulations for managing access to physical spaces. A recent study finds that access control is shifting to mobile and cloud-based solutions, but the merging of physical and logical access control systems still faces many challenges that impede the journey to a truly digital infrastructure experience.

These findings come from a yearly survey of Security and IT professionals on the state of access control technology — its use at their organizations, important trends, and future plans. This survey, conducted in 2020, compares the results of surveys completed in prior years* to reveal trends, challenges, and successes over time.

This year's survey highlights the tension between planning and investing in physical security to combat the evolution of known threats in the face of an unprecedented global pandemic that changed the nature of work. Comparing data between 2020 and prior years, the data indicates that companies are increasingly selecting mobile access as their preferred credential technology, though often in parallel with state-of-the-art smart cards, but still rely on aging legacy and less secure technologies while making the transition. In addition to the current access control system improvements that mobile brings, the top driver to upgrade physical access control was pandemic response.

"Companies can't make the switch to new security technologies overnight, but neither can they afford to rely for too long on aging, vulnerable technology while planning a transition."

-Luc Merredew
HID Global
Regional Marketing Director

Industry Trends in 2021

Access control systems impact everyone in an organization: security professionals, employees, contractors, and visitors. These large systems tend to be static year over year, with changes weighed against business needs and risk profiles. This year saw organizations employing new technology to make physical access administration easier with digital processes, take advantage of features made possible by new technologies, and deploy touchless solutions in response to the pandemic.

"Many of these older technologies — like 125 kHz and magnetic stripe — can be cloned quickly and with minimal technical knowledge."

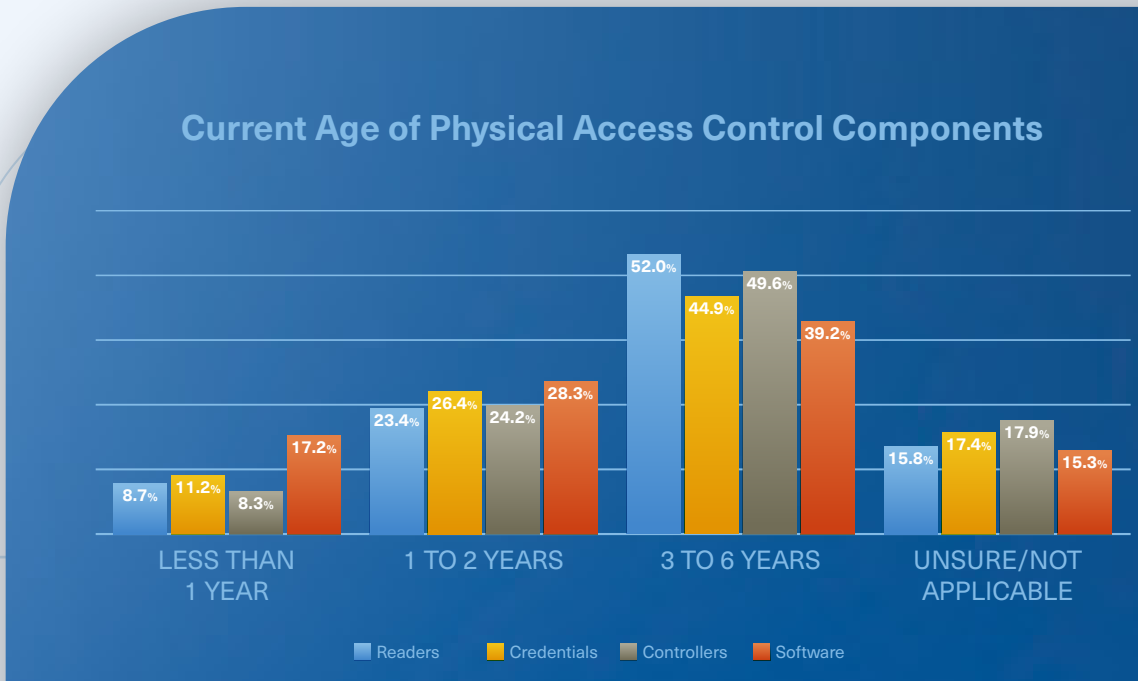
-Luc Merredew
HID Global
Regional Marketing Director

MOVING TO MOBILE, BUT STILL RELYING ON AGING SYSTEMS

Survey results show that over 50 percent of respondents' companies have already upgraded to mobile, are in the process of upgrading to mobile, or have plans to deploy mobile access in the near future. In 2019, only 31 percent of companies were at the same stages of deploying mobile solutions. The industry continues its move toward adopting mobile IDs as secure, convenient credentialing tools. However, as companies make the transition to mobile, they are still relying on legacy and aging access control technology, such as MIFARE Classic.

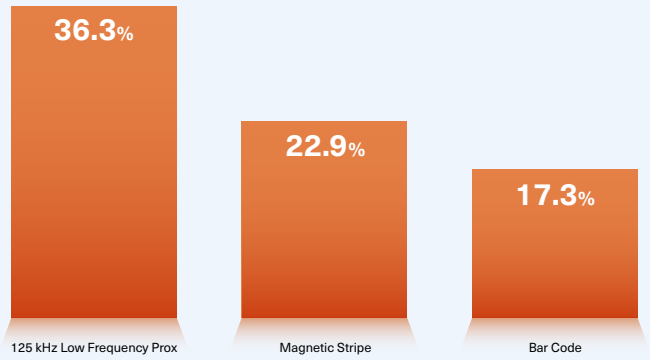
Just over half of the respondents (52 percent) are using reader technology that is not equipped for today's threats or the growing interest in creating more intelligent environments that optimize the workplace and deliver a better user experience. Forty-five percent of companies also reported their credentials are three or more years old, and 50 percent stated their controllers are of similar age. Companies are upgrading to newer software to support their systems, with 39 percent of companies now having software that has been in use for three or more years compared to 48 percent in 2019.

"Security professionals have recognized the value of mobile security solutions and see how it will shape the future of access control," says Henrik Hjelte, HID Mobile Access product marketing manager. "Now, with heightened awareness around the health and security benefits of touchless technologies, companies are starting to replace out-of-date infrastructure with mobile-ready solutions."



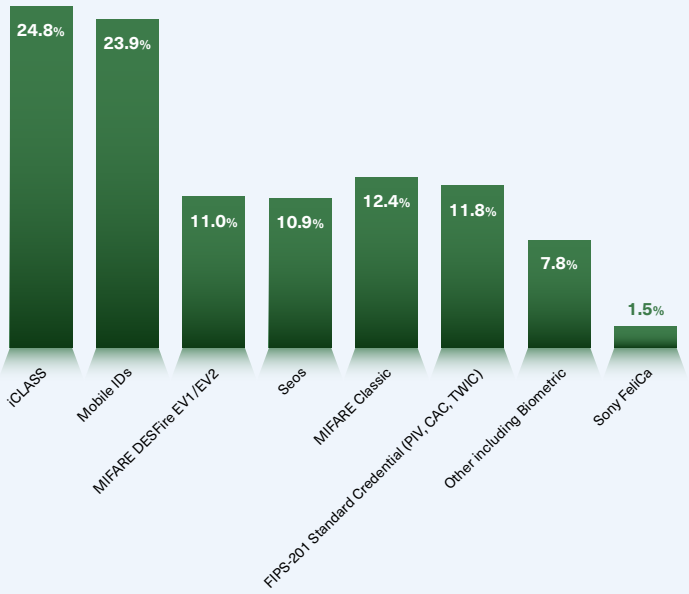
Despite the march toward mobile access, survey respondents indicated that less secure credential technologies are still prevalent in the industry. Thirty-six percent of respondents reported using 125-kHz low-frequency proximity cards, legacy products that offer convenience and reliability but extremely limited security and privacy. Some companies still rely on even older and less secure technology. Twenty-three percent reported using magnetic stripe cards and 17 percent reported using barcode technology. Their continued use exposes organizations to the risk of credential spoofing and cloning, which has been demonstrated widely, and is simple for even the least sophisticated of bad actors.

Less Secure Credential Technolgy Currently in Use



Overall, the industry has seen only incremental improvement with the adoption of more secure technologies. In 2020, 58 percent of reported credentials in use comprise an assortment of encrypted, more secure credential technology such as mobile IDs, Seos®, MIFARE DESFire, iCLASS SE®, biometrics, and other solutions. This is a three percent increase from 2019 and a 12 percent increase from 2017. Most security departments continue to have several access control technologies in use at any given time. With anticipated budget constraints in 2021 and operational challenges from the pandemic, security professionals will be pressed to justify the benefits of upgrading to more secure solutions.

More Secure Credential Technolgy Currently in Use



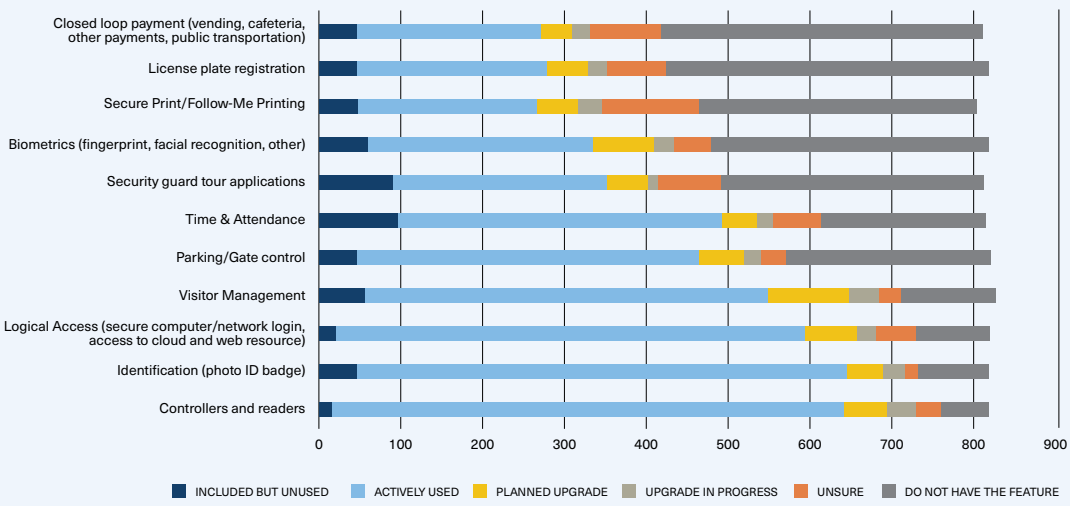
“Companies can’t make the switch to new security technologies overnight, but they neither can they can they afford to rely for too long on aging, vulnerable technology while planning a transition” said Luc Merredew, HID Global regional marketing director. “Many of these older technologies — like 125 kHz and magnetic stripe — can be cloned quickly and with minimal technical knowledge. When companies consider upgrading physical security platforms, they should look to interoperable, future-ready solutions that accommodate any legacy technologies that must be supported during an upgrade. Many companies investing in mobile share this mindset.”

HEALTH AND SAFETY RAISE NEW INDUSTRY CONCERNS

The most common use cases for access control applications shifted slightly in 2020, with respondents citing identification, including photo badges (74 percent in 2020, 80 percent in both 2019 and 2017), logical access to IT resources (70 percent in 2020, 68 percent in 2019, 71 percent in 2017) and visitor management (60 percent in 2020, unmeasured in previous years), which replaces parking and gate control as a top three use case this year. Less frequently used applications, such as closed loop payment (28 percent in 2020, 27 percent in 2019, 24 percent in 2017) and license plate registration (28 percent in 2020, 27 percent in 2019, 25 percent in 2017), remained consistent.

When asked about the top drivers to upgrade physical access control, survey respondents highlighted pandemic response and touchless solutions. Also expressed is a desire to take advantage of applications available in new technologies and make physical access administration easier with digital processes. These drivers converge at mobile technology in access control systems. Mobile access promises convenience, advanced security, and flexibility with the added benefits of enhanced touchless experiences and broader read ranges. Staff, contractors, and visitors are likely to have a personal smart device that is compatible with mobile-based access control technology. Security professionals can provision and revoke credentials over the air, limiting physical contact and improving access control administration with a digital, cloud-based platform.

Access Control System Features Currently in Use



Changes to work and physical spaces introduced new challenges for security professionals. Mobile infrastructure allowed companies that already had deployed the technology to quickly change their security workflows and further encouraged other companies to adopt mobile solutions.

Industry Challenges

The industry trends observed in this year's Physical Access Control survey have their roots in the challenges facing the industry. Emerging threats, vulnerabilities, infrastructure demands of aging technologies, and changes to physical spaces to comply with physically distanced work are pushing organizations to find relevant solutions while overcoming hurdles associated with cost.

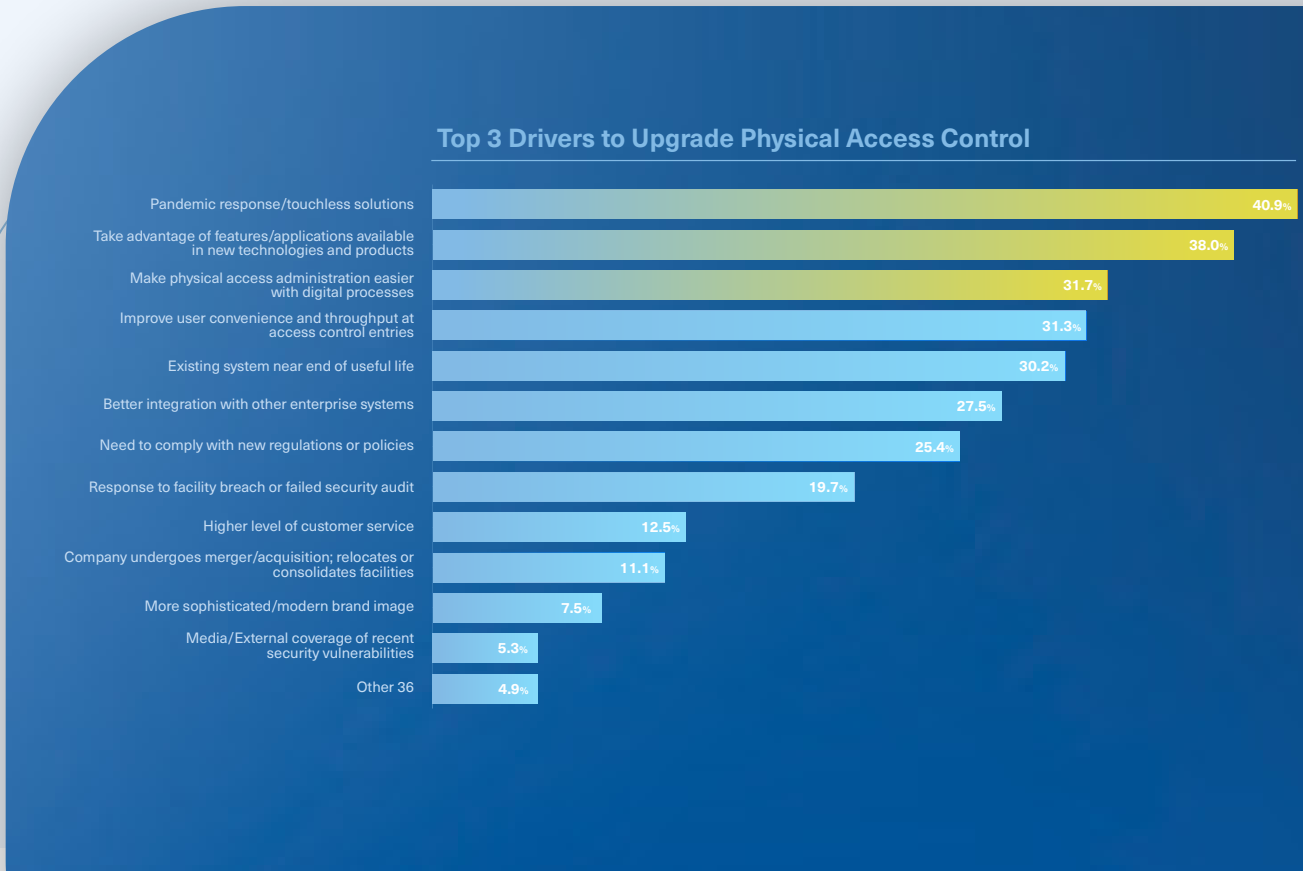
"When companies consider upgrading physical security platforms, they should look to interoperable, future-ready solutions that accommodate any legacy technologies that must be supported during an upgrade. Many companies investing in mobile share this mindset."

-Luc Merredew
HID Global
Regional Marketing Director

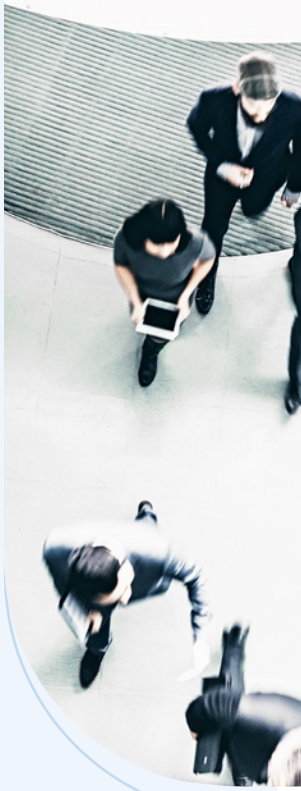
FROM AGING SYSTEMS TO MEETING CURRENT NEEDS

This year's survey asked security directors to choose their top three motivators for upgrading physical access control solutions. The need for touchless solutions topped the list with 41 percent of security directors citing it as a motivator. Few companies were fully prepared for the sudden demand for touchless solutions. Remote credential issuance and a move away from in-person provisioning have encouraged the adoption of cloud-based credential management solutions. And organizations are doubling down on mobile access solutions since the technology leverages an individual's own devices, rather than just a physical badge option or card that must be purchased, distributed, collected, and sanitized.

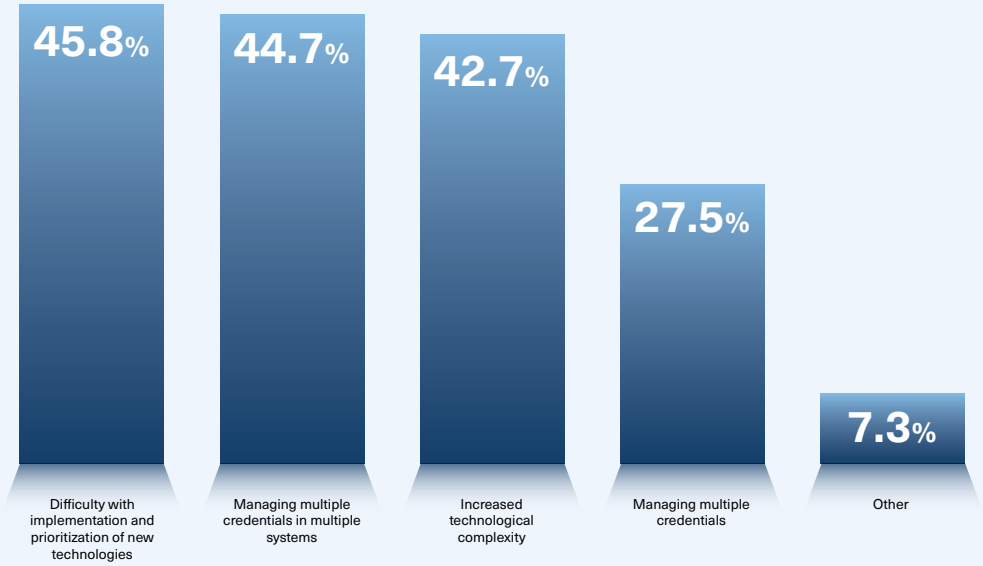
While pandemic response has risen to be the chief access control challenge for security directors, taking advantage of features in new technologies remains a top three challenge from last year to this year. Thirty-eight percent of survey respondents indicated the features and applications available in new technologies as a top driver to upgrade their access control solutions. Building off the advantages of mobile and other touchless solutions in response to health and safety concerns, security directors also seek the advanced security of modern credential and reader systems. Enhanced encryption and biometric solutions are harder to clone or fake. Older systems do not allow for new standards such as Open Supervised Device Protocol or remote credential management.



As the means and motivations of criminals and bad actors continue to advance, security directors are seeking to keep pace. The third most frequently selected motivation for upgrading access infrastructure was the need to make physical access administration easier with digital processes (32 percent). Beyond the advantages of remote credentialing, security directors seek to converge physical access control systems (PACS) and logical access control systems (LACS). Integrating digital processes can lead to more efficient systems, but aging technology can be challenging to merge. The top three concerns with converging PACS and LACS — difficulty with implementation (46 percent), managing multiple credentials in multiple systems (45 percent), and increased technological complexity (43 percent) — must be planned for before an organization retools its secure access infrastructure.

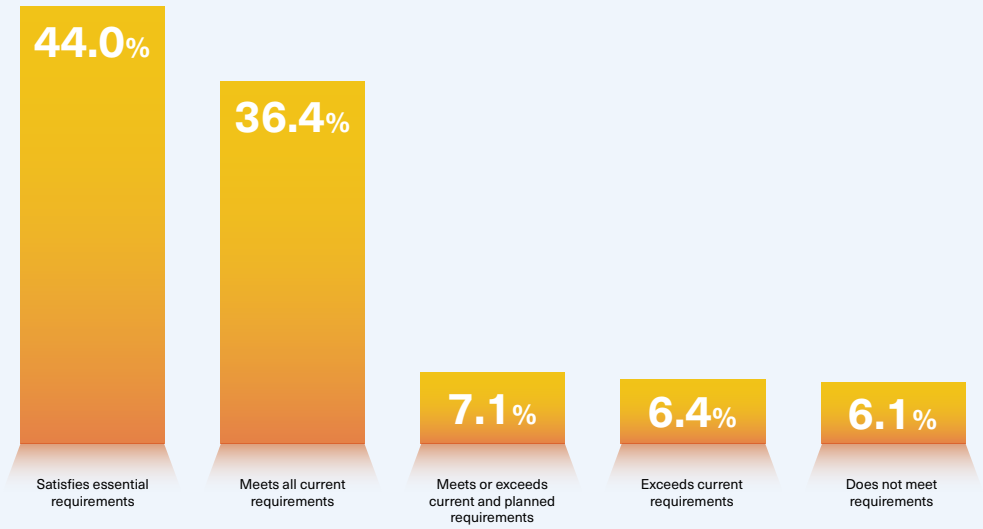


Concerns Surrounding Converged Physical and Logical Access Control



Aging security infrastructure is a consistent challenge that, as threats evolve, continues to erode confidence in security. In 2017, 73 percent of survey respondents reported that their current physical access control solution met or exceeded all current requirements. In 2019, that number fell to 50 percent. This year, it remained at 50 percent. Despite the advancements in secure access technology, many companies still must make do with aging infrastructure. The severity and profile of threats is increasing, while confidence in security is not.

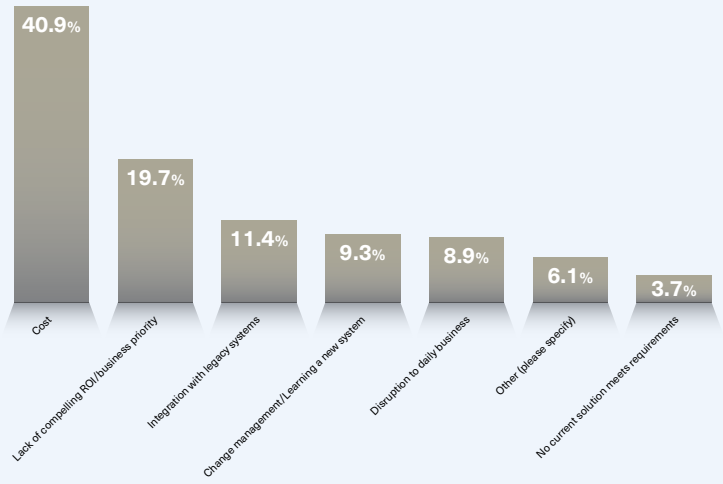
Efficiency With Which Current Access Control Meets Needs



COMMUNICATING THE VALUE OF SECURITY

Forty-one percent of survey respondents cite cost as the biggest obstacle to upgrading physical access control solutions, yet the damage caused by a security breach often has a far greater cost, measured in dollars, loss of brand reputation, or life. Twenty percent of survey respondents said lack of compelling ROI was their main obstacle to upgrading their infrastructure.

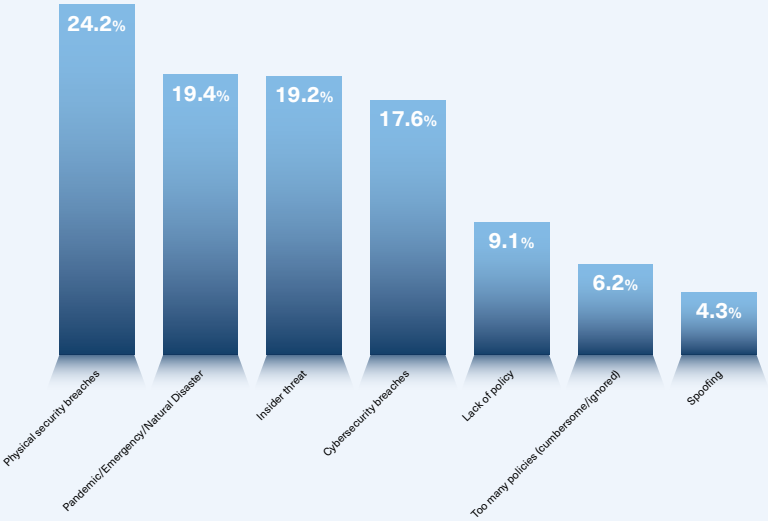
Obstacles to Upgrading Physical Access Control



These figures tell us that executive leadership in some companies continue their struggle to see the value of upgrading their physical access control systems. The industry needs to communicate the value of security without suffering catastrophic attacks. Survey respondents identified the most impactful threats to their organizations as physical security breaches (24 percent), pandemic and natural disasters (19 percent), and insider threats (19 percent). These risks suggest there is opportunity for security professionals to highlight the importance of PACS investments in protecting employees and visitors.

As organizations around the world decide how and when to safely return to the workplace, security professionals have the opportunity to champion the benefits of more secure, touchless solutions. Reducing touchpoints between people and objects is key to protecting employees' health, but the benefits do not end there. Security professionals should communicate the value of solutions that reduce person-to-person contact via over-the-air credentialing and provide real-time building occupancy data to help with social distancing and contact tracing in the event of an infection. Each of these steps will help return employees safely to their workplaces and provide longer term improvements to operational efficiency. While budgets remain constrained, the value of touchless access control solutions may be a catalyst for moving to mobile.

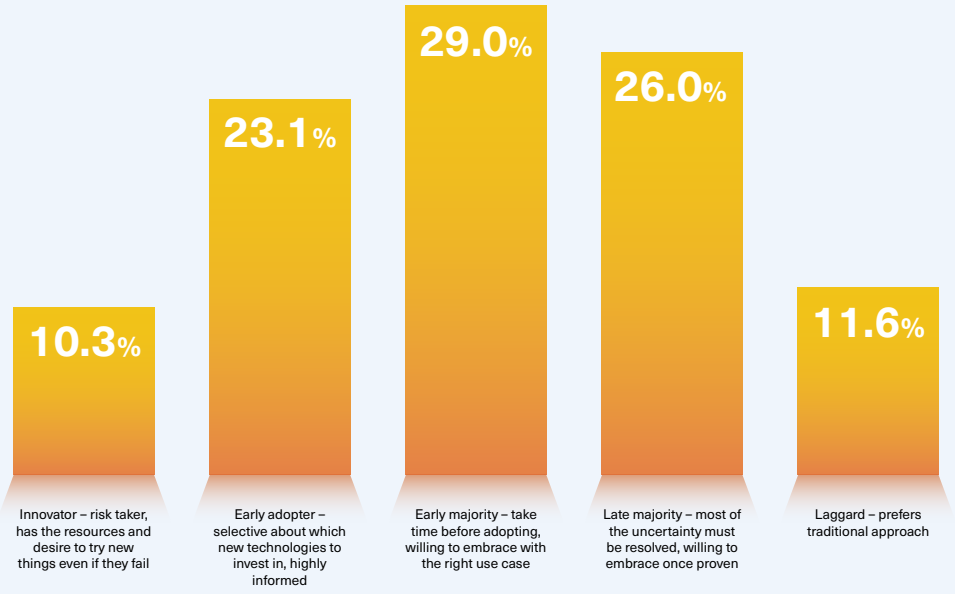
Most Impactful Threat Relating to Access Control Systems



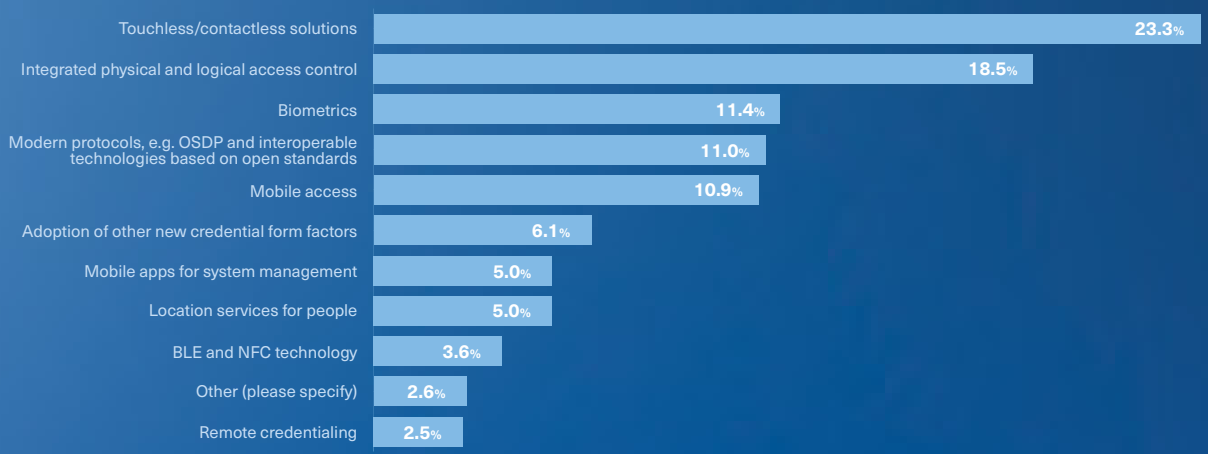
Industry Opportunities

When asked to evaluate where they consider their organization on a technology adoption curve, most survey respondents see their companies as part of the early majority (29 percent), willing to cautiously embrace new technologies for certain use cases, or the late majority (26 percent), willing to embrace new technologies once they are proven and uncertainty is resolved. The security directors see the most impactful technology for access control management as touchless solutions (23 percent), integrated PACS and LACS (19 percent), and biometrics (11 percent). As these technologies mature to a level that companies are comfortable adopting them, they will unlock significant physical access control opportunities.

Access Control Technology Adoption Curve



Most Impactful Technology to Improve Access Control

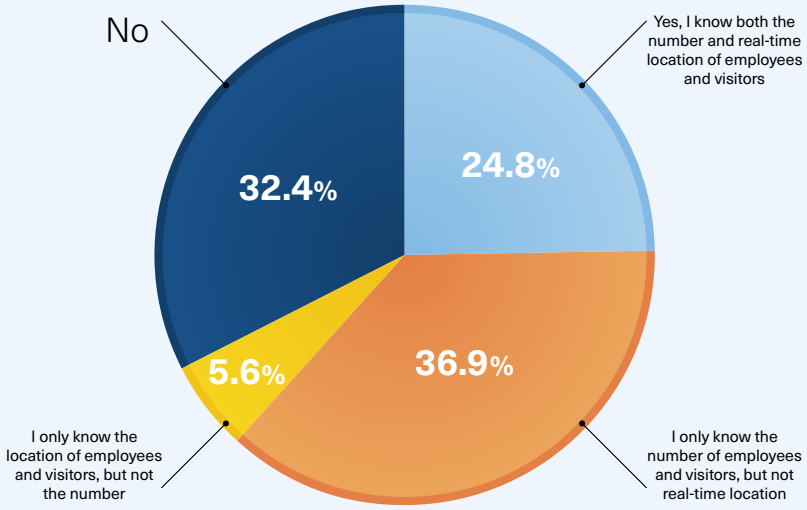


RETURNING TO WORK SAFELY

Security and safety look different now. Security professionals are responding to the current health concerns of the pandemic and designing robust systems to withstand future health and environmental crises.

Survey respondents identify touchless capabilities as the top feature they would require in a new access control system. Touchless solutions are part of creating a convenient, clean access infrastructure, but maintaining new contact tracing and physical distancing requirements necessitates Real-Time Location Services (RTLS). According to the survey, nearly 37 percent of respondents said they knew the number of employees and visitors, but not their location. An additional 32 percent indicated that they did not know the number or real-time location of employees and visitors while on the premises. Twenty-one percent of companies still rely on paper rosters for monitoring visitors, their location, and building usage during their time as a guest in the building, and 16 percent stated having no method at all.

Real-Time Employee & Visitor Location

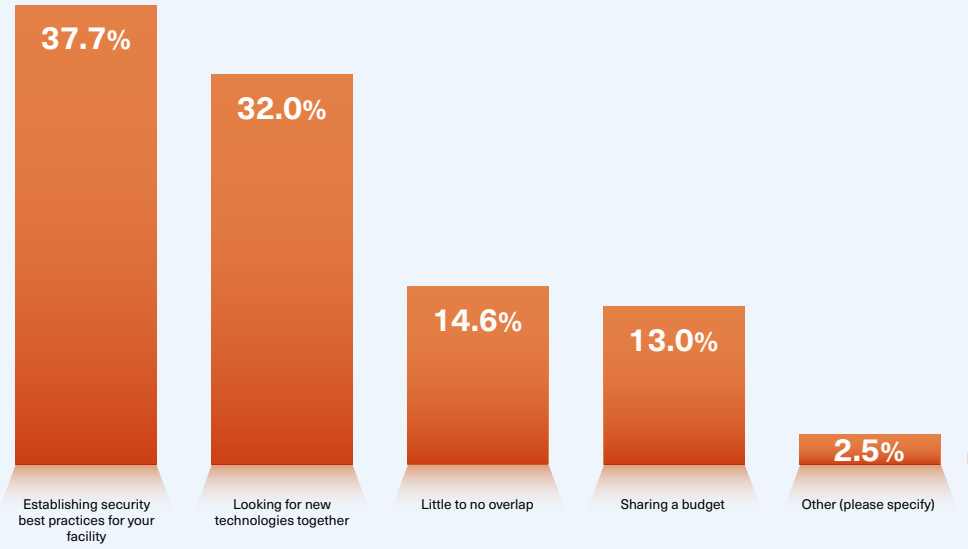


RTLS brings value beyond the near-term return to work. Knowing the number and location of people in a building during an emergency can be invaluable. RTLS systems use RFID, Wi-Fi, or Bluetooth to determine the location of people and items. These systems can work in tandem with access control to protect restricted areas, locate people and assets in an emergency, provide wayfaring to visitors over their smart devices, enable social distancing alerts, and enhance contact tracing efforts in the event of exposure.

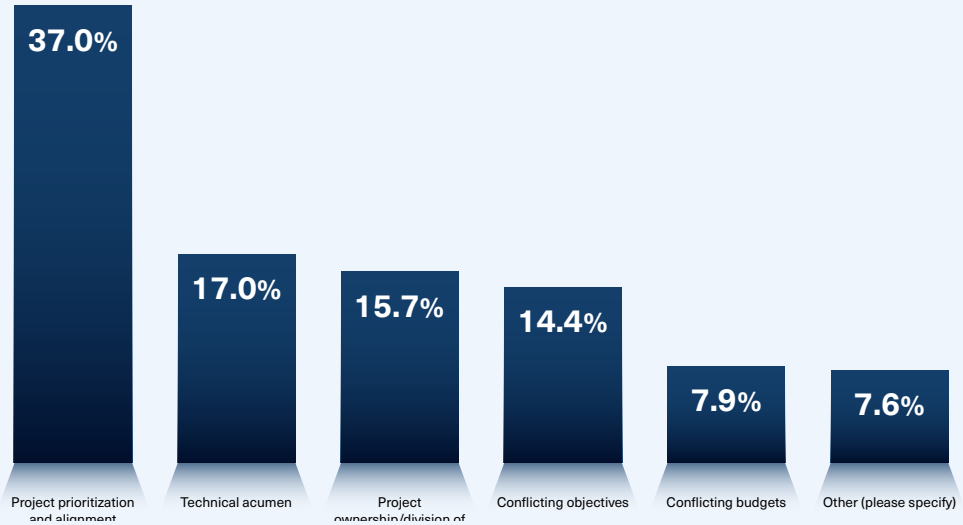
BOLSTERING COLLABORATION WITH IT

Physical security and IT convergence projects are becoming more common, but there appears to be room for improvement in the collaboration between security and IT at most companies. While 61 percent of security directors report working with IT to establish security best practices, which is consistent from the 2019 survey, 52 percent report looking for new technologies together with IT, which is a decrease from 55 percent last year. As physical and logical access technologies become more integrated, companies have an opportunity for collaboration between security and IT. But organizations have work to do. Thirty-seven percent of respondents with security titles listed project prioritization and alignment as the top challenge faced when working with their organizations' IT departments. These numbers suggest that exploring ways to align security and IT may be an opportunity to improve an organization's overall security and IT systems.

How Security and IT Collaborate



Challenges Security Faces Working With IT



"Now, with heightened awareness around the health and security benefits of touchless technologies, companies are starting to replace out-of-date infrastructure with mobile-ready solutions."

-Henrik Hjelte
HID Global
Mobile Access Product Marketing Manager

Moving Toward Secure, Efficient Solutions

The industry is trending toward more secure access control technologies that prioritize user experience and efficient credential management. In 2017, 45 percent of organizations used at least one form of advanced credentialing technologies. In 2019, that number rose to 54 percent. In 2020, 58 percent of organizations had deployed at least one form of more secure credentialing technology. Mobile is the leader in advanced credentialing that puts access control into the hands of employees, contractors and visitors.

While a majority of companies have deployed or plan to deploy new secure solutions, the work is not complete. Threats continue to evolve, and unprecedented events in 2020 revealed new vulnerabilities and demands of security systems. Improvements to secure access infrastructure add multi-application capabilities, introduce easier-to-manage credential options, and more user-friendly technology. Access control technology is poised to protect employees and visitors to companies and restore confidence as they navigate the future of work.

For more information on Access Control Solutions visit
https://www.hidglobal.com/access-control

**The 2020 State of Access Control Report. This report was comprised of survey data collected in 2017 and 2019 and reflect statistics from both years on the single report.*

METHODOLOGY

This report is based on over 1000 responses to the 2020 Access Control Systems Trends Survey conducted by HID Global, ASIS International, and 1105 Media, Inc. in the summer of 2020. A link to the 25-question survey was emailed to Security and IT personnel across a range of titles representing more than a dozen different industries, including Education (11%), Software, Technology & Telecommunications (14%), Government (11%), Manufacturing (12%), Healthcare (8%), and Professional Services (18%). Breakdown of business size is as follows: 31% have fewer than 100 employees, 18% have 101-500 employees, 10% have 501-1,000 employees, 16% have 1,001-5,000 employees, 5% have 5,001-9,999 employees, 8% have 10,000-24,999 employees, and 14% have 25,000 or more employees.

ABOUT HID GLOBAL

HID Global powers the trusted identities of the world's people, places and things. We make it possible for people to transact safely, work productively and travel freely. 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 to navigate their everyday lives, and billions of things are connected through HID technology. We work with governments, educational institutions, hospitals, financial institutions, industrial businesses and some of the most innovative companies on the planet. Headquartered in Austin, Texas, HID Global has over 4,000 employees worldwide and operates international offices that support more than 100 countries. HID Global® is part of ASSA ABLOY.

hidglobal.com

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 9171 1108

2021-01-20-pacs-state-of-access-control-2021-wp-en PLT-05702
Part of ASSA ABLOY