THE STATE OF PHYSICAL ACCESS CONTROL:

IMPACT ON THE ENTERPRISE

HID

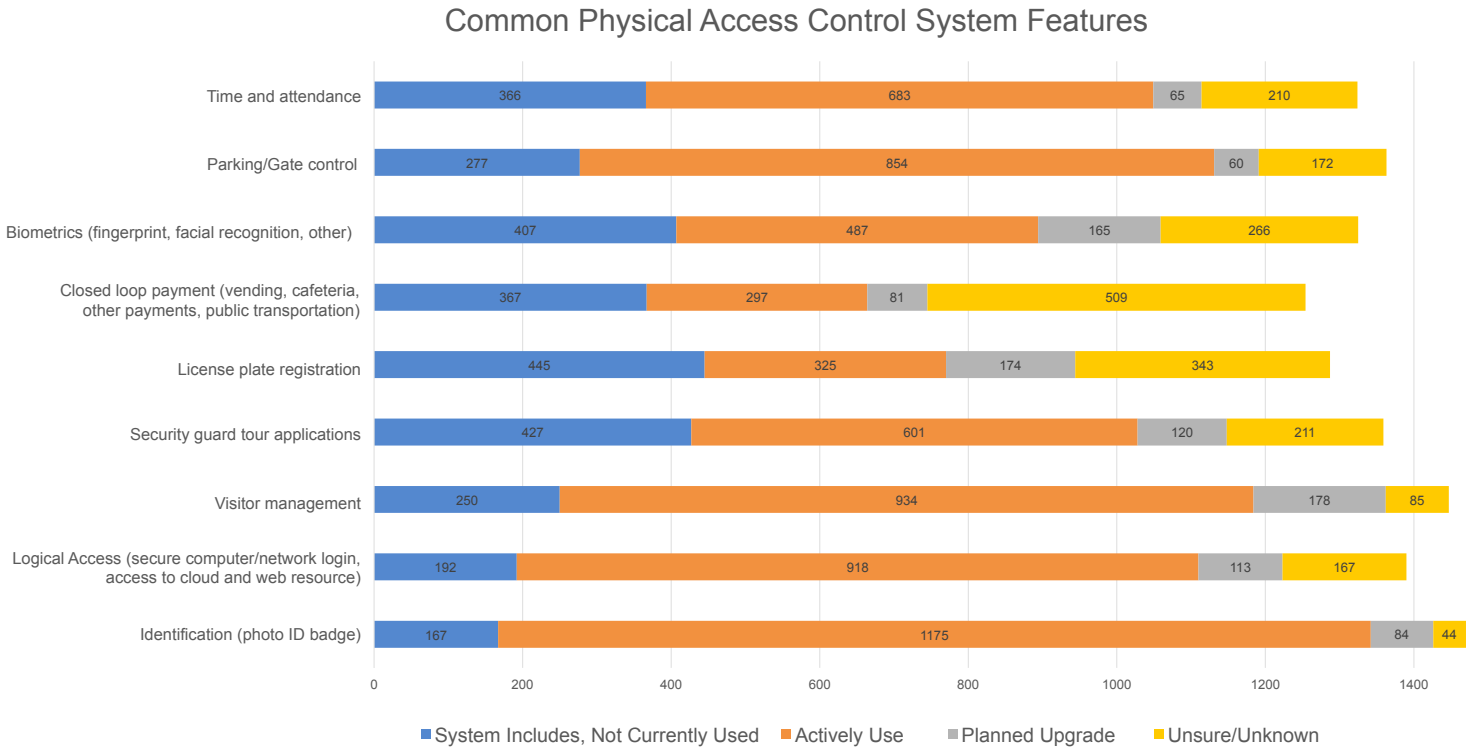
SECURITY MANAGEMENT

The global market for card-based electronic access control (EAC) is projected to reach $10.1 billion by 2020 according to Global Industry Analysts. Recent research by ASIS International, however, finds the technology deployed in the field to be relatively aged and insecure. Responses provided by nearly 2,000 members of ASIS who serve as security directors or consultants indicate the most common access control credential technology deployed today is 125 kHz low frequency proximity, which is relied on by 44 percent of respondents, while 33 percent use magnetic stripe, 21 percent barcode, and 10 percent MIFARE Classic. Just 45 percent of respondents indicated use of more secure technologies such as FIPS-201, iCLASS, MIFARE DESFire, Seos, and Sony FeliCa.

The most common technology in use—125 kHz proximity—was introduced more than 25 years ago. These contactless cards offer extraordinary reliability and longevity. They have no batteries to fail, relying instead on radio frequency (RF) signals sent out from the reader. The cards themselves simply consist of an antenna, a capacitor, and a chip that stores the card's ID number.

This read-only technology is very economical but has widely-known security vulnerabilities. This technology will keep incidental visitors out but will not withstand anyone with an intent to breach the system. "Cards can easily be cloned, even without the holder's knowledge, and the cloned card can then be used to open any door available to the original holder," says Daniel Bailin, Vice President, Strategic Business Development and Innovation with HID Global. There is also no direct means of determining if a system has been compromised, essentially worsening matters by providing a false sense of security. "If someone clones a card and comes into the building, you won't know because it looks like a legitimate entry," says Bailin.

One-third of respondents indicated the use of magnetic stripe cards—the same technology that is currently being phased out of credit cards in favor of chips due to its lack of security. Magnetic stripe cards have information stored on a thin strip of magnetic tape that is subject to wear with every use. Magstripe remains a popular technology in the university setting where its early capacity to serve as a common denominator between systems earned early market share in that setting. It can serve as a single creden-



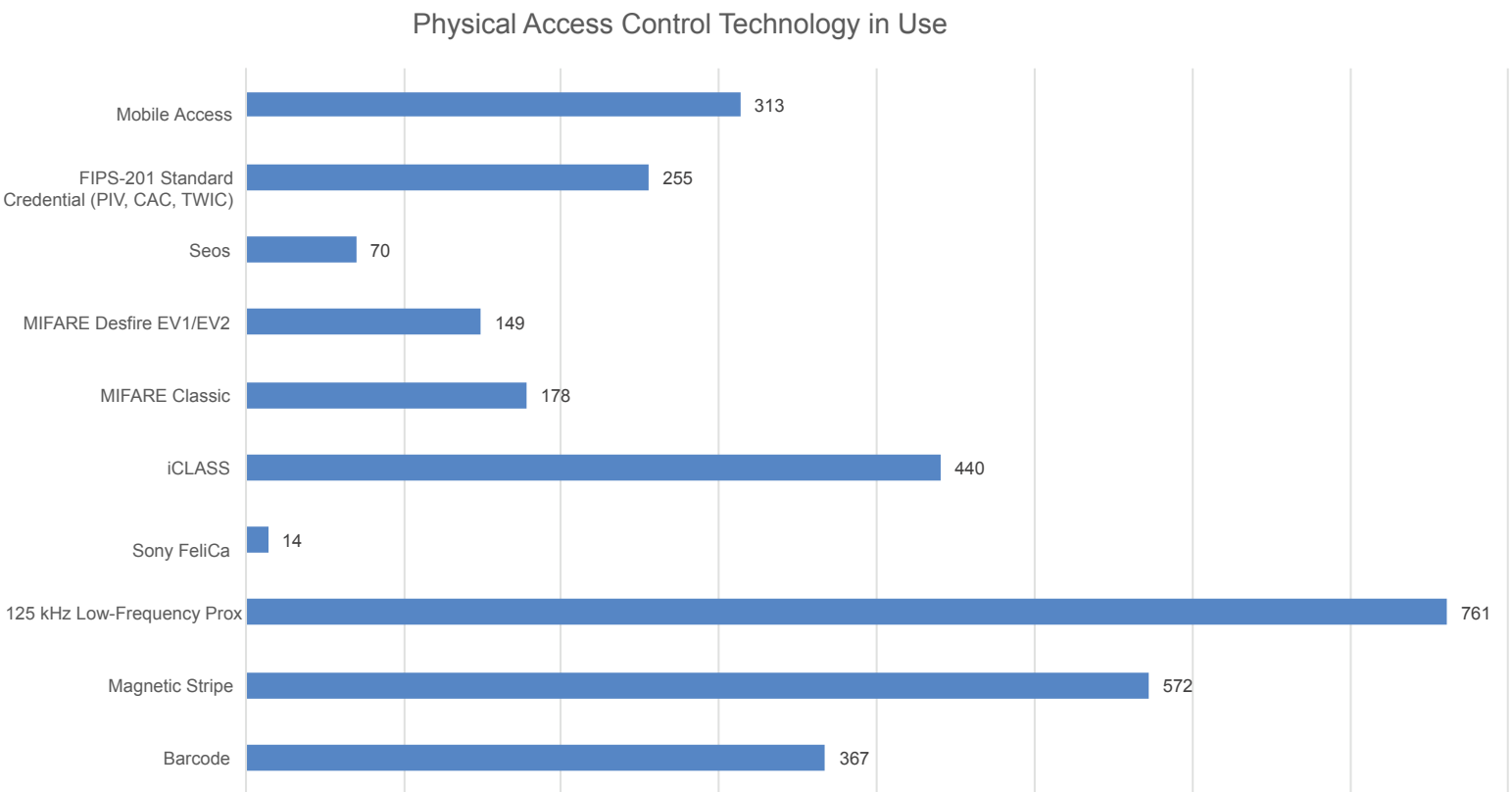
tial that grants access to the dorm, enables bookstore transactions, and stores meal plan data. Magstripe can also frequently be found in hospitals and enterprise environments.

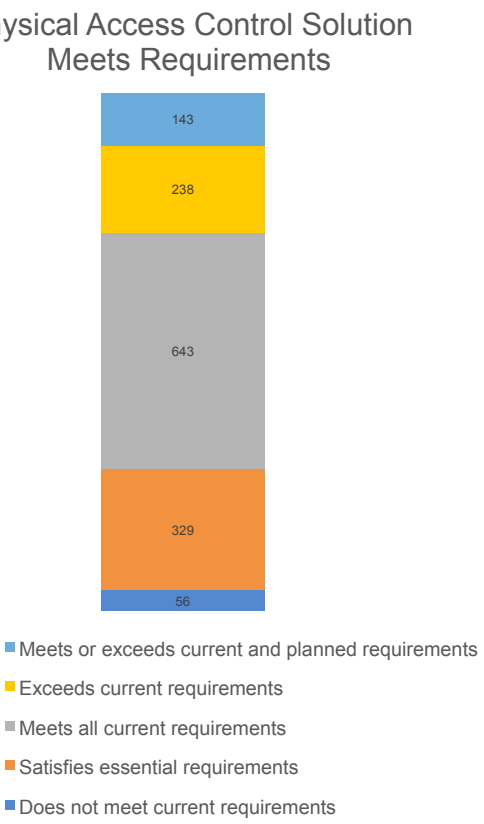
"Unfortunately it's horribly insecure," says Bailin. "Generally speaking there is no security associated with magstripe because the data is all stored in plain text without encryption. In fact, it is the lack of encryption and security that makes it so easy to use across all of those systems." Bailin does grant that magstripe is somewhat more secure than proximity cards because cloning a magstripe card would require someone to take physical possession of the card. Proximity cards can be cloned by simply getting close enough to a person to ask directions or hand out a flier.

Approximately one quarter of respondents rely on iCLASS, a contactless smart card technology that was introduced in 2003. With both encryption and mutual authentication, iCLASS cards are more secure than 125 kHz proximity cards. They also offer far more flexibility with the capacity to support biometrics, time and attendance, and general office functions such as access to company printers. Beginning in 2013, iCLASS was upgraded to iCLASS SE, which added additional layers of encryption and digital signatures to further improve the security.

Barcode access cards, still used by one in five respondents, is the least secure credential on the market. The technology is still common on library cards and grocery store loyalty cards but has never been suitable for securing facilities. Because the security element is clearly visible, the system can easily be defeated by simply copying with a standard copy machine or taking a picture of an existing card.

The 13.56 MHz MIFARE Classic—used by 10 percent of respondents—essentially introduced encryption to the access control market. MIFARE Classic also offers the capability to load additional applications to the card. In 2008 MIFARE Classic was attacked and broken by researchers and the results made public. It is still often used for transit where the values are small,





but can easily be cloned when used for access control.

MIFARE DESFire—used by 9 percent of respondents—offers both improved flexibility and improved security using more modern encryption technology.

Many organizations choose cards that offer dual technology, combining technologies to provide a transitional stage between legacy systems and modern access control technology. Proximity/Smart Cards are a typical hybrid solution in which sensitive areas of buildings or entire facilities may be upgraded immediately while areas of lower concern such as cafeterias and restrooms may wait for years.

Near Field Communications (NFC) is a technology still relatively new to the security industry and it is getting tremendous attention due to its use on mobile phones. To be clear, the NFC specs do not include any security models and rely on the same RFID low level protocols as the legacy technologies such as MIFARE Classic. Bluetooth, still nascent in the security space, is another technology commonly found on mobile phones and many wearable devices. Bluetooth is ubiquitous and open standard, flexible, low cost, and features low power requirements.

Seos is a credential technology that uses best-in-class cryptography to provide access control credentials. These can be implemented as traditional RFID cards, as well as in both NFC and Bluetooth mobile phone applications. The technology is device-agnostic (card and mobile). When implemented as a mobile credential, it is supported on both iOS and Android platforms. It can be found in new installations in enterprise and university environments. Seos fulfills many of the promises of universal credentialing to include physical and logical access, payment, and government identification. “One of the design objectives with Seos was to be independent of the token (chip or phone) technology and independent of the contactless pipe used,” says HID’s Bailin.

MOVEMENT TOWARDS MOBILE

Just as credential technologies have evolved over the years, so have the ways users interact with them. One of the bigger developments over the past few years has been the increased adoption of mobile credentials, which allows users to access facilities via their

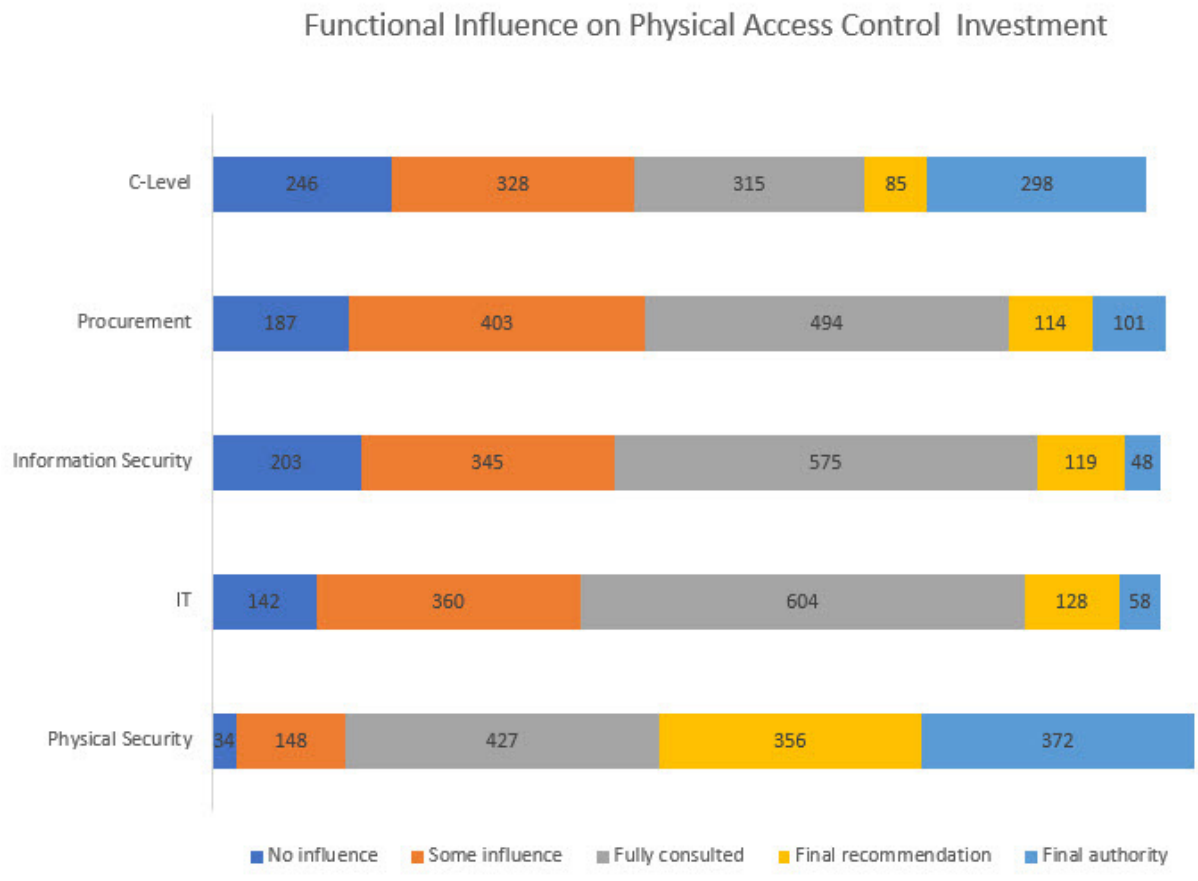
mobile device. Approximately 20 percent of survey respondents indicate they have upgraded to mobile-enabled readers or are in the process of doing so. Another 34 percent will upgrade to mobile-enabled readers within the next three years. Overall, 77 percent of those surveyed said that mobile credentials will either improve or somewhat improve their overall access control system.

The move to mobile seems natural for many organizations, because it can heighten user convenience, streamline credential management, and improve security. Employees rarely, if ever, leave their mobile device at home, making it a natural supplement to smart cards. For security professionals, provisioning and de-provisioning credentials can be immediately performed over the air, which increases efficiencies and reduces vulnerabilities.

By 2020, IHS predicts that 20 percent of all credentials will be mobile. For this to become reality, organizations will have to assess their existing technology and build plans to incorporate mobile into their access control ecosystem.

EXPANDING ACCESS CONTROL WHILE CONVERGING BUDGETS

While the industry remains slow to upgrade systems that have proven reliable and largely maintenance free, one key driver for updating has been converging multiple building infrastructure systems so that the effectiveness of each is improved. From a strict security standpoint, says Bailin, "Would your system allow a person to log on to their desktop computer if they have not used their access card to get through the front door?" Respondents indicate cards are commonly used for more than just physical access. Access cards are used as photo IDs by 82 percent of respondents, visitor management by 66 percent, logical access by 67 percent, parking/gate control by 63 percent, and time and attendance by 52 percent. Substantial numbers also report using cards for guard



tour applications, and closed loop payment systems.

Not only are traditional access cards enabling increased technological convergence, organizations are now merging access control budgets within IT and security departments. Survey respondents indicate decisions to upgrade physical access control solutions include a high level of participation across the enterprise. Twenty-eight percent of respondents indicate the IT department influences the process, 47 percent report the IT department is fully consulted in decisions, and another 10 percent indicate that the IT department makes the final recommendation.

The responsibility for making final recommendations and the final authority for physical access control infrastructure still falls more to physical security than to any other area, as may be expected, but this plurality is less than 30 percent. The easy observations that technology forges a convergence of physical and IT security have become cliché, but perhaps too little attention has been paid to the fact that the profession of security in the enterprise is far more collaborative than it was in years past.

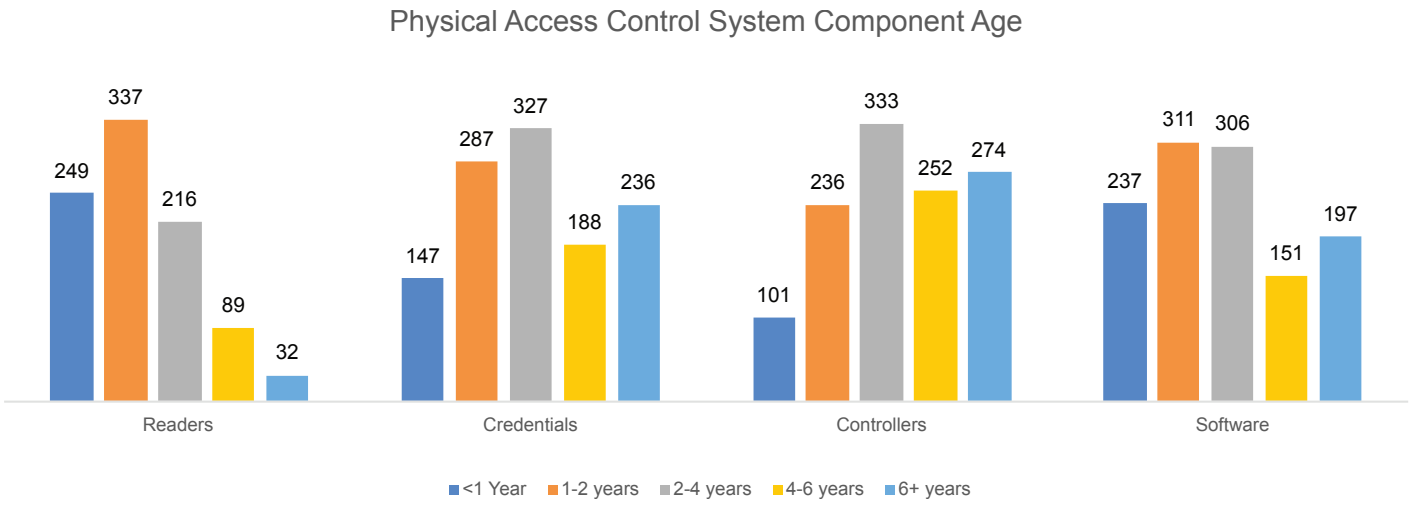
"Part of the challenge in the security world has been that success was measured by the absence of bad things happening," says Bailin. "If it ain't broke, don't fix it, so there wasn't much motivation to try new things." To a large degree this explains why proximity and magstripe are still so prominent, even though they are known to be insecure. "In the absence of something bad happening," says Bailin, "real vulnerabilities are often perceived as just theoretical."

Obsolescence can come in many forms as risk grows quietly but incessantly. Collectively, however, the rate of technological adaptation in the market raises important questions and concerns.

THE FUTURE ON OUR DOORSTEP

No technology stands alone in today's interconnected and interdependent business environment. Each technology is part of a vast ecosystem that grows increasingly networked every day. One example is access to large offices in major cities. "If you go to any high-rise building in Manhattan at 8:30 in the morning, there can be 10, 12, or 15 security turnstiles," says Bailin. "Nobody likes turnstiles. Not the architects, not the tenants, and certainly not the visitors."

Typically a visitor will have to go to a security or information desk and present identification that can be checked against the log. That process may take only a few minutes, but when these visitors arrive simultaneously as they do in peak periods, they begin to stack up and they begin to be late for appointments or miss meetings entirely. In this instance the technology and the process of visitor management—an



essential security element—is having a negative impact on the organization's success. And this is where adopting new technology can make an impact that is felt in the C-suite.

"Potentially, credentials can be sent remotely to a visitor's phone, even providing directions such as telling them to use turnstile number three, go to elevator number five and take it to floor number seven," says Bailin. "Imagine the before-and-after picture of a high-rise lobby when such a technology is installed. Viewed from the visitor's perspective, this is simple and a real convenience. From the point of view of the enterprise, there's real value in improving the efficiency of the operation."

The decision-making process behind investing in such infrastructure is not taken in the context of access control alone; it also considers modern building automation. The property manager for that high-rise is looking for solutions to manage every aspect of the property: security, HVAC, elevator maintenance, and lighting. All of these systems converge to improve the capacity to manage the building. Decisions are often driven by the objective of being aware of who is in the building and being responsive to that population. While the impact on security and usability are clear, the bottom-line reality is this allows for more efficient use of energy and substantial return on investment.

That is where security directors need to be, not just thinking of access control as a means of security portals but as part of managing people in the environment, improving their experience, enhancing security, and contributing to the bottom line as part of an integrated building management approach.

METHODOLOGY

ASIS International invited members to participate in an online survey on their use of physical access control systems and technologies in November 2016. Of the 1,897 respondents, 59 percent were security managers or directors, 30 percent were security consultants, 4 percent were company executives, 4 percent were facility managers and 3 percent were information security or IT directors. ■