RESEARCH REPORT

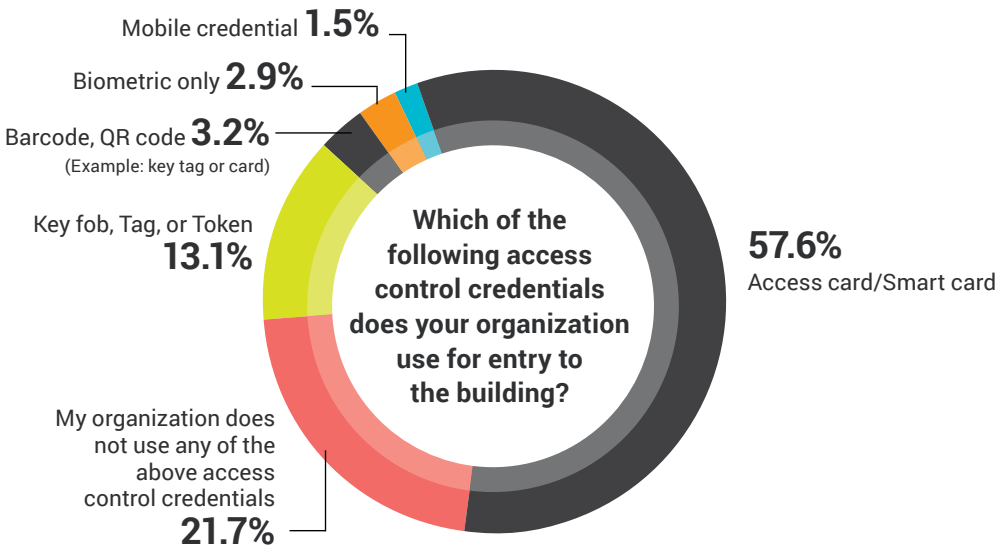
ACCESS CONTROL IN PRACTICE FACES TECHNICAL, WORKPLACE AND USER CHALLENGES

HID

New opportunities exist for security leaders to improve day-to-day use

Recent research shows most access control technology currently in use is not as secure or convenient as many security managers believe, according to day-to-day users of the system. Furthermore, responses provided by more than 1,600 managers, directors, analysts, and senior managers in a survey conducted by The 05 Group found 22 percent of organizations do not use any methods of electronic access control, further exposing these businesses to potential breaches.

The survey also found that 58 percent of respondents use access/smart cards, and 13 percent use key fobs, tags, or tokens as their primary method of access control. Approximately 8 percent use another method, such as a barcode, QR code, mobile credential, or biometric access. But the majority of these access control methods use low-frequency RFID technology, which poses real – and rarely documented – security threats to organizations where they are still in use. The technology may keep incidental visitors out, but cannot bear the pressure of anyone intent on a breach.



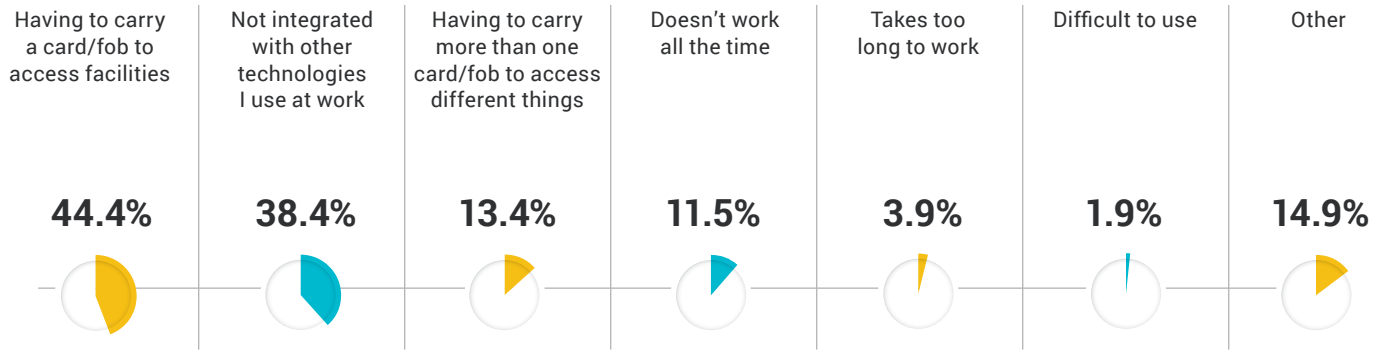
"In the absence of something bad happening, real vulnerabilities are often perceived as just theoretical," says Daniel Bailin, Vice President, Strategic Business Development and Innovation with HID Global. But significant threats can arise from system, technology, and policy shortcomings. Survey results found that while users desire more convenient access control methods and extended capabilities, there remains a lack of understanding and adherence surrounding the importance of policy and security protocols. This leaves significant opportunity for threats to become real incidents that can wreak havoc on an organization. Additionally, many organizations lack significant training and onboarding procedures that can be implemented to help educate employees on best practices for access management.

Convenience: Credential Holders Demand More

While security managers are primarily concerned with keeping a facility secure through strong solutions and robust policies and procedures, users of access control systems desire convenience.

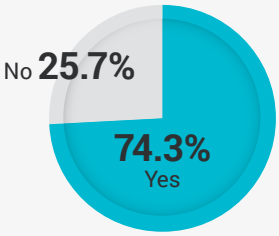
The main objection of respondents to their organization's current access control system is having to carry a card/fob to access the facility (44 percent), followed by the lack of integration with other technologies used at work (38 percent). For example, more than half would like to use their credentials for network login (50 percent) and individual computer login (55 percent) to help streamline access to the tools they use every day.

What don't you like about your organization's current access control system? **(Select all that apply)**

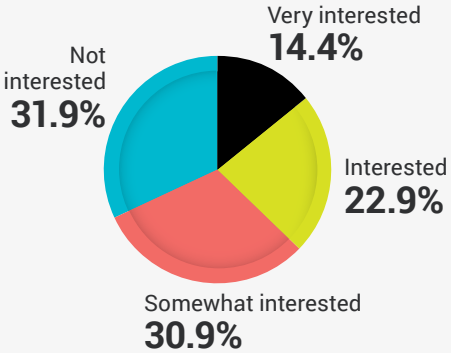


In addition, users want more credential options. Most employees (68 percent) are interested in accessing facilities via their smartphones. Approximately 74 percent of employees already use mobile phones for work purposes, so relying on them for access means carrying one less item. Unlike other form factors, users do not view carrying their mobile phones as a burden and instead consider it an important extension of themselves.

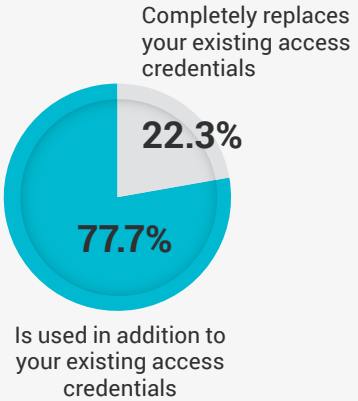
Do you use a mobile device for company business?



Would you be interested in having your access credentials on your mobile device?



Would you prefer that your mobile device:



"Many companies rely on more than 20-year-old access control technology that is easy to clone: It can be done in less than five seconds," states Luc Merredew, Product Marketing Director, Physical Access Control, Americas at HID Global.

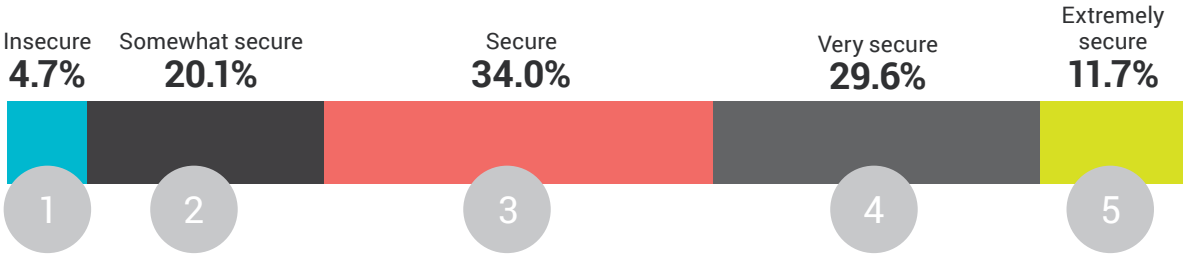
The majority (78 percent) of those favoring mobile credentials would prefer the solution offered as an option rather than the only way to enter a building. In this case, the phone and the card would act as backups to each other which maximizes the chances of employees being able to successfully enter the building. Interestingly enough, mobile was not a popular stand-alone solution, as 32 percent of respondents do not want to use only mobile systems for authentication. This means that many employees prefer multiple options for authentication instead of a winner-takes-all approach that is seen in more traditional access control offerings.

Overwhelmingly, users want ease of use (77 percent) and reliability (51 percent) out of their organization's current access control systems, followed by security (40 percent). However, legacy access control solutions pose a significant security risk, opening an organization to potential breaches. But there are ways for security managers to deliver the convenience desired by employees while strengthening the security posture of the organization.

Security: Perceptions Are Not Based in Technical Reality

While the majority of employees trust their organization's access control systems (75 percent), there is evidence to suggest that the systems are not as secure as they might think. In many instances, this is due to an organization's reliance on access control technology that is decades old or has been deployed in an insecure manner. A recent survey from ASIS International found that more than three out of four enterprises depend on legacy technology that fails to meet modern security standards and best practices. The survey found that the most commonly used systems are 125 kHz low frequency proximity cards (Prox) (44 percent) and magnetic stripe cards (Magstripe) (33 percent). These legacy systems are invariably vulnerable to a number of basic attack vectors using information and technology that is readily available online.

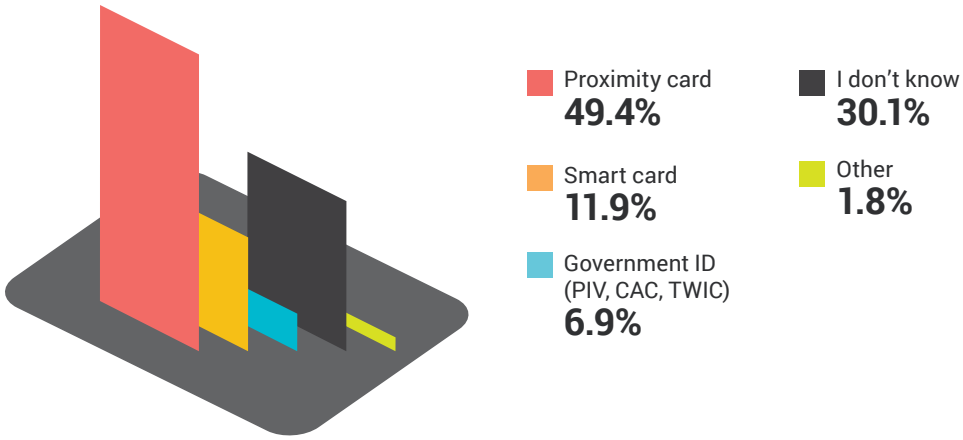
Based on your organization's existing access control system, on a scale from 1 to 5 with 5 being "Extremely secure", how would you rate your building's security?



Many organizations are using outdated technology, such as first generation radio frequency identification (RFID) products, which consist of an antenna and simple chip that stores the credential's ID number. These products have no data security features, like encryption. While suited to keeping incidental visitors out of a facility, this approach will not withstand individuals with the intention to breach the system as the credential can easily be cloned without the holder's knowledge. That cloned credential can then be used to open any door available to the original holder.

"We have seen a number of instances in higher education environments where students copied legacy technologies, like proximity cards, and gained access to restricted areas or services, such as dorm rooms, vending machines, dining hall payment systems, and even faculty offices," says HID Global's Merredew. There is often no direct means of determining whether a system has been compromised, which means many security leaders may have no indication of a breach until after the incident has occurred.

Do you know what technology is used on the access card that you use?



Magstripe solutions also present intruders with low security barriers. Introduced in the 1960s, their technical details are well documented, and the encoded data is completely unprotected. Off-the-shelf devices and Web-based services enable criminals to create duplicates of these cards. In fact, the technology has become so outdated it has been replaced for more than a decade in Europe.

As evidence of its security limitations, magstripe technology is currently being widely phased out of credit cards and replaced with EMV chip card security, which is designed to prevent fraud. Much like chip cards are used for payments, modern access control cards use secure microprocessor hardware chips to protect the user's identity, using sophisticated but fast encryption.

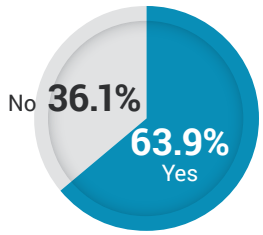
Policy: Ineffective Access Control Policies Plague Organizations

While outdated technology still plays a significant role in facility security, there is also evidence that a lack of clear access control policies, including a degree of apathy about the role access control plays in keeping an organization safe, still burden many organizations.

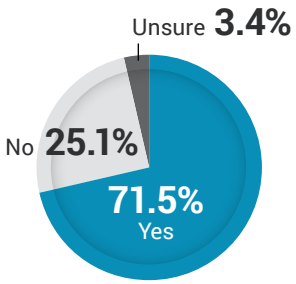
One of the core features of an ID-1 card format (credit card sized) credential is the potential to mark the card with company information or person-specific details like a name and photograph. While not all cards are printable; the use of a printer with compatible credentials allows fast, high quality on-site ID badge personalization.

USERS WITH THEIR PICTURE PRINTED ON THEIR CREDENTIAL

Is your picture printed on your access credentials?



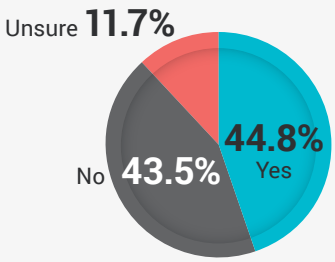
Does your organization have a policy regarding requirements to wear your access credentials while in the facility?



USERS WITHOUT THEIR PICTURE PRINTED ON THEIR CREDENTIAL

Does your organization have an access control policy?

(Example: Employees must keep their credentials on their person at all times)



The majority of respondents whose picture is printed on their card or badge (71.5 percent) report that their organization has an access control policy which includes wearing their credential while in the facility. This number is significantly lower (45 percent) for those without their picture printed on their credential. Additionally, an equal number (44 percent) of respondents without a printed picture report no policy at all with another 11.7 percent unsure if a policy is in place.

"At its core, a policy that effectively communicates the identity management policies of an organization is critical to its success, providing core objectives for onboarding employees, granting permissions, and tracking a user's activities to better manage operations," says Merredew. "But it is evident there is a disconnect between the use and implementation of policies that govern access control."

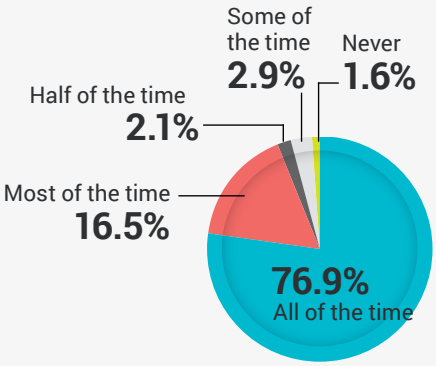
For those organizations that have access control policies in place, the communication of these policies is overwhelmingly positive, with 91 percent of respondents reporting that the company policies were thoroughly communicated to them. While 45 percent of respondents claim that they never see policy violations made by fellow employees, close to 30 percent of employees see their colleagues not abiding by the policies in place on a daily basis. Another 14 percent see violations once a week, while still another 14 percent witness monthly violations.

Despite these frequent violations, an overwhelming amount of employees (80 percent) did not report violations witnessed to management, which means the challenge for organizations lies in the encouragement of protocol adherence. One irony here is employees' perception about themselves, as 94 percent claim to follow corporate directives all or most of the time.

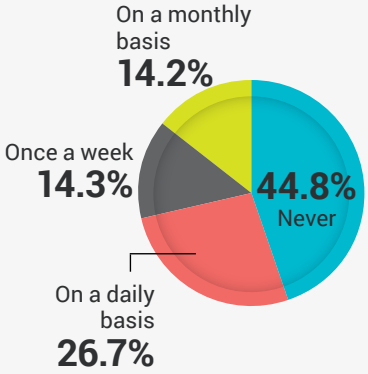
More specifically, according to the research, 47 percent of respondents report having a policy for "tailgating," or going through an entry on someone else's credentials, yet 61 percent reported viewing coworkers violate these policies. However, more than half of respondents (53 percent) claimed their organization does not have a policy in place for tailgating.

Almost one-third of respondents have no idea what kind of technology is used on the access card they use every day, which means there is significant opportunity for security managers to provide more training to users on best practices for access. The research supports this, as the majority (63

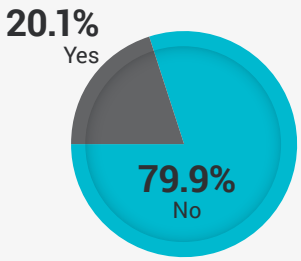
How often do you abide by your company's access control policy?



How often do you see others NOT abiding by this policy?



Have you ever reported someone that did NOT abide by this policy?



percent) reported that very little effort was required to receive access control credentials; and 74 percent said it took less than a day to receive their credentials. Organizations can improve the process by teaming human resources with security managers to optimize onboarding procedures that explain the importance of security in general. They can also develop best practices for caring for and keeping track of credentials inside and outside of a facility in an effort to reduce loss and potential theft.

Users also find current access control systems only somewhat convenient (45 percent), which may contribute to their lack of adherence to access control policies. The top criticism from 44 percent of respondents is that they feel burdened carrying their credentials. During the workday, they are worn around their necks (26 percent), kept in their purses or wallets (21 percent), worn on their belts (18 percent), kept in their pockets (14 percent), or clipped to shirts or jackets (13 percent). Outside of work, credentials are placed in a wallet or purse (33 percent), at home (30 percent), in a briefcase (20 percent), or in the car (15 percent). The credentials are not viewed as an inherent part of their person but instead an inconvenient add-on. As a result, many workers, approximately 42 percent, forget to bring their credentials to work during the year.

Security leaders are tasked with managing the habits and preferences of users, including employees, partners, and visitors to a facility, and as such, these entities must be factored into a comprehensive approach to access control. As evidenced in the research, technology is only as good as the people behind it. At times, processes are often overlooked out of convenience, which can dismantle enterprise-wide protections. Leaders can work to overcome these challenges by providing the best possible user experience through smooth authentication mechanisms, built-in safeguards against possible bad actors aiming to gain access to an organization's critical data, and empowering users with the tools they need to navigate the system easily in the event of an incident.

Why Upgrading Can Benefit Enterprises

More than ever, security managers are tasked with improving operations and the security of an organization by finding and implementing new and emerging technology. The decision-making process takes into account both cost and usability of a solution, and leaders must weigh the two while simultaneously examining policies and procedures that govern the day-to-day usage of the technology.

According to recent research from IHS Markit, an estimated 4.5 million mobile credentials were downloaded in 2016. The market research firm predicts that this number is expected to increase to 136 million in 2020, indicating a significant increase in the integration between mobile devices and access control solutions as a means to provide better value for end users.

Upgrades made to existing access control technology can lead to increased efficiencies and a focus on managing people in the environment, improving their experience, enhancing a facility's security, and contributing to a comprehensive approach to building management. There are a number of ways security managers can provide upgraded technology and increased convenience to employees through access control systems that offer mobile credentials, capabilities for extended applications, and multi-factor authentication.

Mobile devices are one such technology emerging in the market today. According to recent research from IHS Markit, an estimated 4.5 million mobile credentials were downloaded in 2016. The market research firm predicts that this number is expected to increase to 136 million in 2020, indicating a significant increase in the integration between mobile devices and access control solutions as a means to provide better value for end users.

Users also want technology that can be used in multiple ways, with 38 percent complaining that legacy technology acts in a standalone fashion. Many modern access control systems boast the ability for multiple departments to collaborate using updated software that can integrate with workforce management solutions to eliminate employee time theft and increase identification accuracy and reliability. A more modern access control solution offers users the ability to centrally manage mobile identities from a single platform, leading to improved productivity. For example, once HR enrolls a new staff member, the organization's access control system is automatically updated to include a new user. Once this is done, security managers are alerted of a new employee and can start the procedures for issuing credentials. Similarly, in the event of a lost, stolen, or compromised credential, IDs can be revoked remotely through the centrally managed platform. What once could take more than 24 hours, now takes a matter of minutes, saving on data entry time, the possibility of user error, and lag time that can lead to potentially dangerous situations.

Modern access control systems can also extend capabilities beyond physical access control. Employees have the potential to use their building access credentials for other applications, such as logging into the enterprise network, accessing corporate applications, cashless vending, and supporting secure printing in classified areas. The research supports this assertion, as 62 percent of respondents would be interested in having these types of capabilities.

Advanced credential technologies not only improve convenience for workers but also for system administrators. Many of today's organizations are under pressure to reduce security costs and increase ROI. As many new access control systems are easily upgradable, and select solutions are compatible with existing systems, the majority of updates can be made through software without significant investments in hardware. As a result, enterprises do not have to remove and replace an existing system to add capabilities, such as secure printing, making the business case to apply capital investments to the new technology.

Finally, many existing systems rely on single factor authentication, which is normally sufficient for general entries and standard work areas, but may be deemed insufficient for secure areas like labs, HR record storage, or server rooms. By adding multi-factor authentication, a higher assurance level can be gained. For example, adding a keypad allows a physical card (something the employee has) to be supplemented with a PIN (something the employee knows). Or, a biometric reader can be added, which combines a fingerprint or iris scan (something the employee "is") to a standard credential.

Conclusion

Employees demand convenience from an organization's access control system, with the added desire to use a single tool to better integrate with a facility's other technologies. But they also share the ultimate goal with security managers of increased security, which is why the majority of organizations should not wait to implement significant upgrades to outdated, legacy technology that is present in many of today's facilities. Additionally, security managers must be diligent in their approach to develop policies that help educate employees on best practices for the use of access control within the organization.

Modern access control solutions not only have the ability to bolster the overall security posture of an organization; they also are multifaceted in their approach to work seamlessly with multiple departments in an effort to streamline operations, provide better standard operating procedures for users, and allow almost immediate action to be taken in the event of a breach. It is critical for security managers to step away from a siloed approach to security and instead look for ways to connect devices and solutions in a cohesive way to better deliver results. •

METHODOLOGY

The 05 Group surveyed 1,693 individuals, representing more than a dozen different industries, including education (21 percent), manufacturing (13 percent), information technology (12 percent), health services (12 percent), and security, professional and business services (8 percent). Of the respondents, 27 percent were managers, 16 percent were analysts/associates, 13 percent were directors, 10 percent were senior managers, and 5 percent were business owners. Breakdown of business size is as follows: 28 percent have less than 100 employees, 21 percent have 101-500 employees, 8 percent have 501-1,000 employees, and 16 percent have 1,001-5,000 employees.