ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

THE ESSENTIALS OF ACCESS CONTROL

INSIGHTS, BENCHMARKS, AND BEST PRACTICES

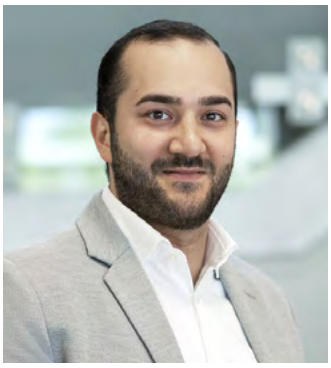
Sponsored by

FacilityOS

CONTENTS

Revision: This file was updated in April 2025 to reflect sponsor name change from iLobby to FacilityOS.

MAKING PROGRESS IN AN EVER-CHANGING ENVIRONMENT



FacilityOS, formerly iLobby, is honored to partner with ASIS for another comprehensive market report. Much like our previous collaboration on Security Practices in Visitor and Emergency Management, this report delivers vital insights for security pro-fessionals, cementing our commitment to enhancing security standards and serving as a dependable resource for the ASIS community.

Given the rapid progress in access control technology, the corresponding challenges and risks are evolving equally. Our collaboration with ASIS offers a deep dive into where organizations stand today with respect to access control capabilities and highlights key measures for its optimal deployment.
As you prepare to read this report, I want to highlight a few pivotal findings that stood out for me which I encourage you to keep in mind while reading.

First, access control has been found to be a highly effective tool, with 93 percent of organizations declaring it an essential piece of their broader risk management or security plan. Furthermore, over 70 percent of organizations that have implemented access control systems have reported no more than five serious incidents within a year. This empowers security professionals to maintain a notably higher level of confidence in maintaining an exceptionally low incident rate within their organizations.

With such strong results in favor of the value of access control, a surprising 39 percent of organizations still employ manual systems like pen and paper to manage visitor credentials. While there is a certain charm to tradition, the mounting intricacies of modern security demands advocate for a shift. It is promising to note that 41 percent of these firms are eager to transition to a digital solution, signaling a visible trend in the sector.

The findings in this report reinforce that the convergence of security data is becoming a staple in sophisticated programs at large multinationals and global organizations. Our data indicates a clear trend towards heightened integration: 54 percent of organizations have merged their access control with video monitoring, while another 42 percent have integrated it with visitor management systems. Such interlinking not only offers a rich view of security events but also expedites threat response.

Beyond its informative value, this report charts an ambitious yet attainable course for security programs, highlighting the significance of data-driven decisions. With the security field in constant motion, having foresight and remaining adaptable is paramount. To the global organizations reading this: envision this report as your means of navigating uncharted waters. Aligning your security initiatives with its findings will ensure enduring resilience for your organization. On behalf of FacilityOS and our partners, we thank you for taking the time to read this report.

–Ariel Mashiyev
Chairman & CEO
FacilityOS

EXECUTIVE SUMMARY

Any successful security framework must have at its heart a competent, highly functional access control system. In this context—and in the context for this whole report—an access control system refers to the combination of technology and security policies (also called processes and procedures) used to permit access to people with permission to be at a location and deny access to others. The study endeavored to benchmark the access control technology and policies in use and assess their effectiveness.

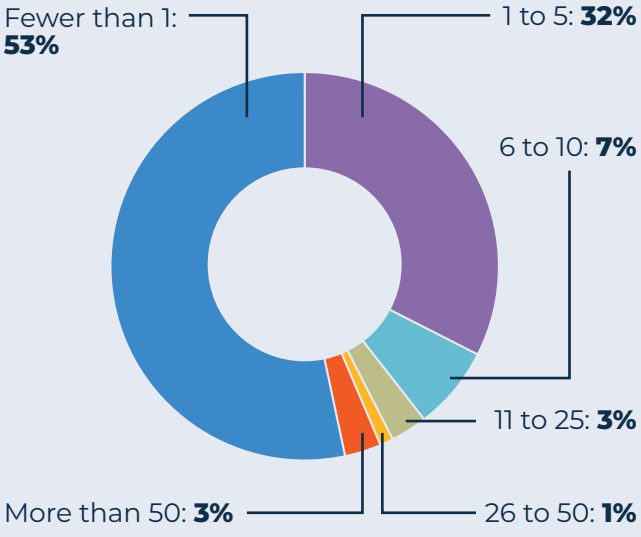
The survey provided a wealth of information and, coupled with several interviews of security professionals and experts, yielded four key findings and a host of benchmarks the security profession can use, starting with the chief finding: access control systems are highly effective.

KEY FINDING 1: ACCESS CONTROL SYSTEMS ARE HIGHLY EFFECTIVE

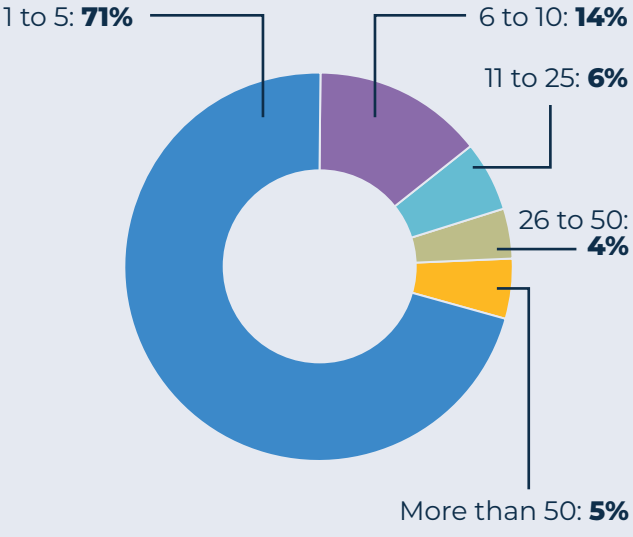
Getting straight at the heart of the matter, the survey asked security professionals about access control incidents in a couple of ways. First, it tried to assess how commonly access control incidents occur, asking this specific question: "How many security incidents related to access control or unauthorized physical access do you face per week on average? (An 'incident' is anything that requires security to take extra action to investigate or remediate.)" The choices started with "Fewer than 1" and increased in categories up to "More than 50."

Filtering out those who said they did not know, 85 percent said they average five or fewer inci-

Chart 1: Access Control Incidents Requiring a Security Response Per Week



Access Control or Unauthorized Physical Access: Serious Incidents Per Year



dents per week. Researchers expected to have to crosstab this question with organization size to arrive at workable conclusions. However, there were so few respondents who reported six or more incidents there was no need (see Chart 1).

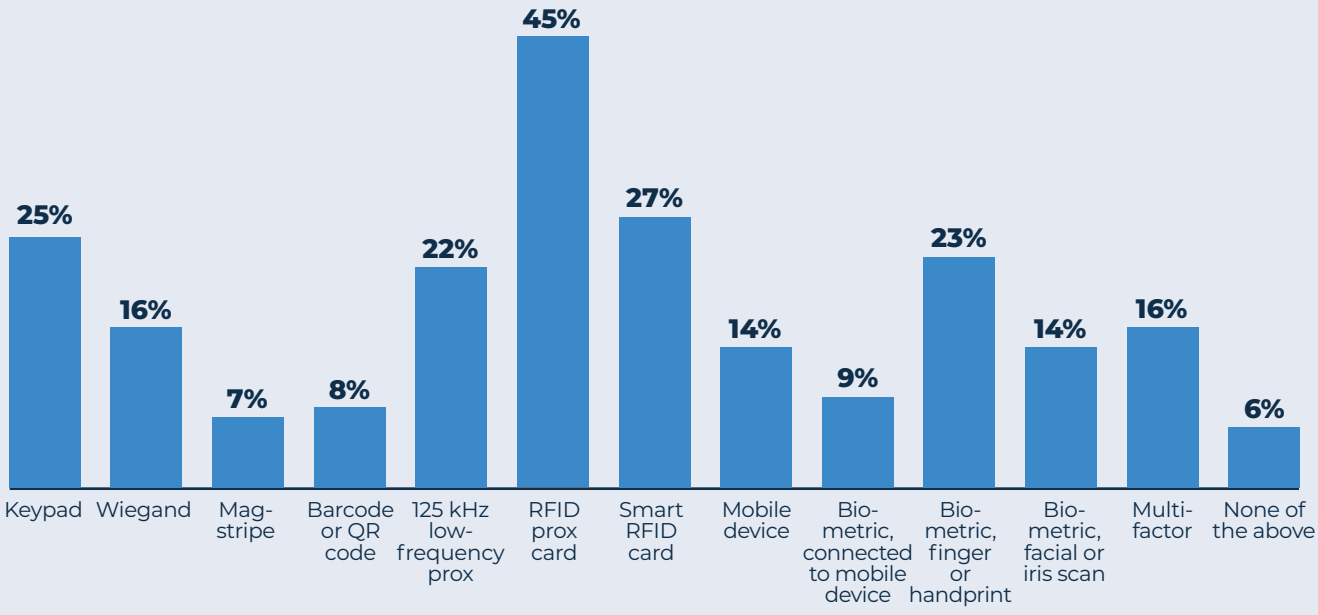
The survey also asked "how many critical or serious access control or unauthorized physical access incidents do you face each year?" Researchers left it to participants to decide what constituted a "serious" incident. Still, the results were remarkably consistent with the weekly results: Fully 71 percent said they faced no more than five serious incidents and a total of 85 percent had fewer than 10 incidents.

Taken together, the two results show that access control systems are remarkably effective, and this is despite the myriad ways they could be compromised, from technology failure to sabotage to human error. One likely reason for access control system effectiveness is because 93 percent of respondents reported that access control was an explicit part of a broader risk management or security plan—universally believed to be an absolute necessity among the security consultants and security professionals interviewed for this report.

However, proving that there is always room for improvement, the survey listed types of common access control failures and asked security professionals if they had experienced any of them in the previous six months. Only 8 percent had not experienced any of them. Tailgating or piggybacking topped the list, with 61 percent reporting the issue, followed by propped doors, an issue 50 percent faced in the prior six months. Of the incidents listed, fake or stolen credentials (8 percent) and breaking and entering (15 percent) were encountered with less frequency.

In addition, more than 70 security consultants and security solution providers took a special survey documenting their opinions. Though a small sample size, the results to the question,

Chart 2: Access Control Credentialing Technology in Use



"Do you think companies place too much or not enough emphasis on access control solutions?" show a notable response: two-thirds said companies did not emphasize it enough, while 30 percent gauged the amount of emphasis as about right.

KEY FINDING 2: COMPANIES ARE SHIFTING TO MORE SECURE TECHNOLOGY

The survey asked security professionals to select all the types of access control technology they employed and provided 12 methods to choose from (see Chart 2). Several of the types are known to have security deficiencies. Access control solutions using 125 kHz low-frequency proximity cards became ubiquitous when the previous king of access card technology, Wiegand magstripe cards, was shown to be easily bypassed or the cards spoofed. Unfortunately, several years after low-frequency cards supplanted Wiegand cards as the gold standard of security access credentials, severe security vulnerabilities of low-frequency cards became widely known. Anyone who could purchase $100 worth of equipment, do 20 minutes of internet research, and put forth a little reconnaissance effort could easily bypass low-frequency card controls.

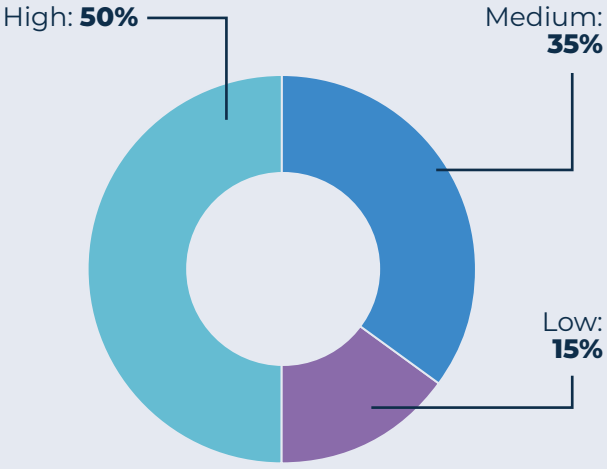
The good news is: use of the least secure access control technologies is declining. A 2019 study from ASIS showed that 51 percent of respondents used 125 kHz low-frequency proximity cards. That number declined to 22 percent in this study. Likewise, use of magstripes fell from 26 percent to 7 percent.

Researchers categorized the list of credentials into three categories, acknowledging that this categorization is a generalization only, and will not cover all use cases. The breakdown is as follows:

Security Level	Credential Type
Low	Keypad; Wiegand; Mag-stripe; Barcode or QR Code; 125 kHz low-frequency prox
Medium	RFID prox card; Smart RFID card
High	Mobile Device; Biometric (all types); Multifactor

Because many organizations will employ multiple types of access credentials depending on their analysis of their needs, researchers analyzed all survey responses and recategorized them. Those who only used credential types with a low security level fell into the low category. Those who used medium security level credentials—whether only using medium level methods or a combination of medium and low security levels—were reclassified as medium. Similarly, those using high security level credentials fell into the high category (see Chart 3).

Chart 3: Percent Who Rely on Low-Security Technology vs. Have Higher-Security-Level Technology in Use



KEY FINDING 3: VISITOR MANAGEMENT PLAYS A CRITICAL ROLE

The number of access control variables related to visitor management are numerous. Organizations must account for such varied situations as a vendor or customer coming to a facility for a one-hour meeting to regular contractors coming multiple times per week (such as custodial contractors) to a repair contractor coming for a couple of days to a long-term contractor filling in for several days or weeks. The survey asked several questions about the technology used to support visitor management as well as policies in place and effectiveness measures.

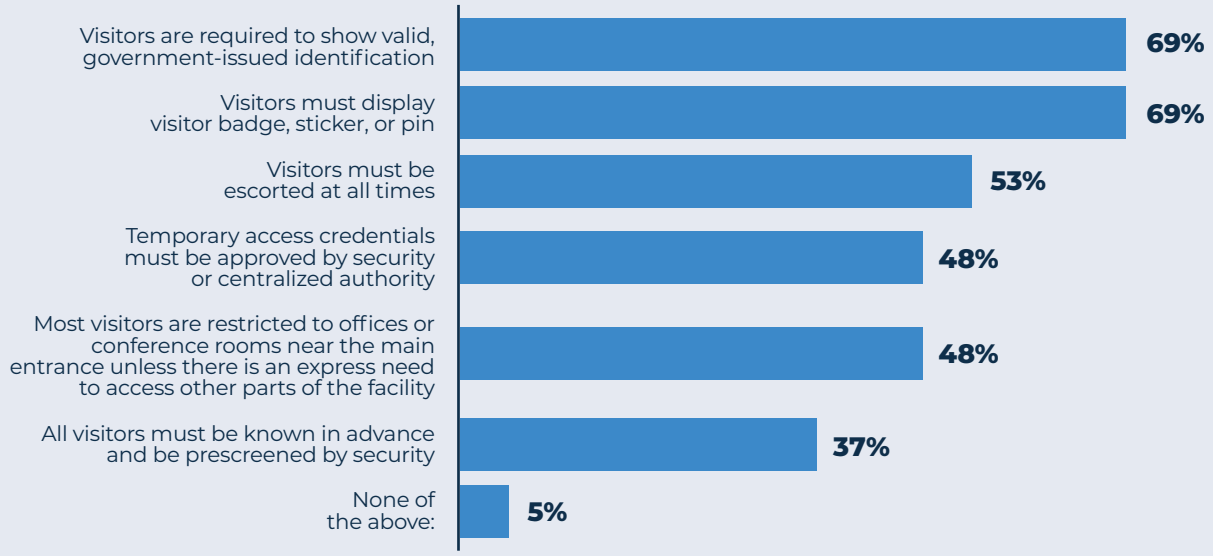
On the technology question, 39 percent reported that they use a manual system, such as pen and paper or a spreadsheet, to keep track of temporary credentials issued to visitors. Fifteen percent said they did not issue temporary credentials. (See Chart 19 in the full report, page 23, for a more detailed examination of how temporary credentials are issued.) Of these groups, 41 percent said implementing a dedicated digital system to track temporary access credentials is part of an upgrade plan.

The survey also asked about visitor policies in place. Requiring visitors to show identification is a common policy, with 69 percent of security professionals saying their organization had the policy. Less ubiquitous, but still heavily used, 37 percent said all visitors must be known in advance and prescreened by security (see Chart 4).

KEY FINDING 4: INTEGRATING WITH OTHER SYSTEMS IS VITAL FOR ACCESS CONTROL EFFECTIVENESS

The benefits of linking surveillance systems and access control is both obvious and very much in practice. Asked to select from a list of nine security features—from cameras to receptionists to locked doors—that their company employs at primary entrances, video surveillance inside (85 percent) and outside (84 percent) were by far the most used. In addition, when asked how they ensure their access control systems had not been breached, 76 percent of security

Chart 4: Visitor Management Policies and Practices



professionals said they actively monitored video surveillance.

The survey asked which technologies were integrated with access control technology, and once again the video surveillance system topped the list, with 54 percent reporting that video and access control technology were integrated (see Chart 5). Other systems often tied to access control technology include visitor management (42 percent) and time and attendance software (31 percent). Emergency management systems and tying access control credentials into logical IT systems access were less frequently integrated.

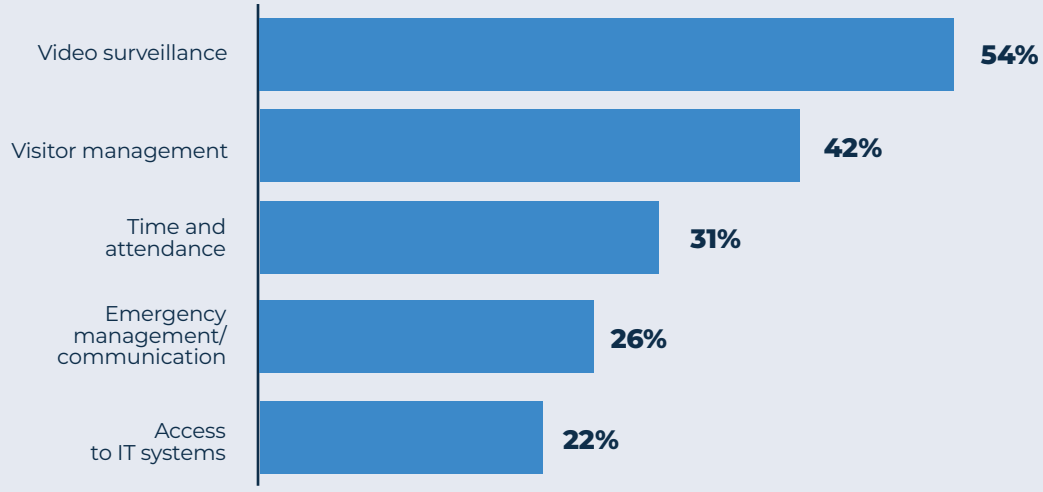
In the consultant's survey, security consultants were asked to rank the importance of seven different technological innovations related to access control. Given a 10-point scale, the consultants gave very few rankings below a five, or a "medium level of importance." So, while everything scored highly, "access control integration with surveillance system" made top marks, averaging an 8.63 (and 40 percent ranking it a nine or a ten). The next highest average ranking was 7.99, given to "linking access controls to critical systems such as IT access." This compared to an average score of 7.85 for "using multifactor authentication for access control," and a 6.48 for "artificial intelligence or machine learning analysis of access control data." Again, all the innovations scored highly, but the two on integrations scored the highest.

METHODOLOGY

This report is based primarily on an access control survey deployed via SurveyMonkey in September 2023. The survey was promoted to ASIS members and customers via email and through ASIS newsletters and social channels. No attempt was made to widen participation beyond these outreach methods.

A total of 1,022 participants answered at least some questions. All survey data collected is

Chart 5: Technology Systems that Are Integrated with Access Control Technology



reported, including from survey participants that did not complete the entire survey. Not all survey participants saw all the questions depending on how they answered previous questions. Of the questions that most survey participants saw (or would have seen if they did not abandon the survey), the lowest number of responses was 664. For most questions outside the consultant survey described below, the margin of error is ±4 percent at the 95 percent confidence level.

One of the demographic questions asked participants to choose a title that closest fit their current situation. Fourteen percent, or 140, of the participants chose either "I am a security consultant," or "I am in a nonsecurity role at a company with products and services that aid a company's security." These participants were then given the option of answering the same questions the security professionals were asked or of answering questions geared at consultants and business partners. Sixty percent chose to answer as consultants, 71 total participants answered most of the consultant survey questions. The responses to these questions should be viewed as rough guides only because they carry an estimated margin of error of ±10 percent at a 90 percent confidence interval.

Survey development was led by ASIS staff, and included advice from two security consultants, one security professional, and one representative from the survey sponsor, FacilityOS, formerly iLobby. In addition, ASIS staff interviewed two security consultants and two security professionals after the survey to aid in analysis and provide context for the findings.

The full survey and results are presented as summary data in Addendum. Overall, the demographic information is in line with previous ASIS research in terms of location, organization size, and industry of participants. Approximately half of respondents were from North America; Africa, at 13 percent, was slightly higher than other ASIS surveys while Europe, at seven percent, was slightly lower than other surveys.

FULL REPORT

The full report presents demographic information from survey participants and is followed by sections on each of the four key findings described in the Executive Summary. Much of the same information—both exposition and presentation of data—is repeated in the full report.

Additional related benchmarks and supporting information beyond what is presented in the Executive Summary, as well as contextual descriptions provided by qualitative interviews and open-ended survey questions, is presented in the full report sections.

Finally, the full report highlights some interesting findings that did not fit neatly into the four key findings classifications, as well as a short discourse on access control topics that were not covered, or were undercovered, in the survey, as well as topics that bear watching in the future.

WHO TOOK THE SURVEY?

Readers can find the complete set of demographic results in Addendum.

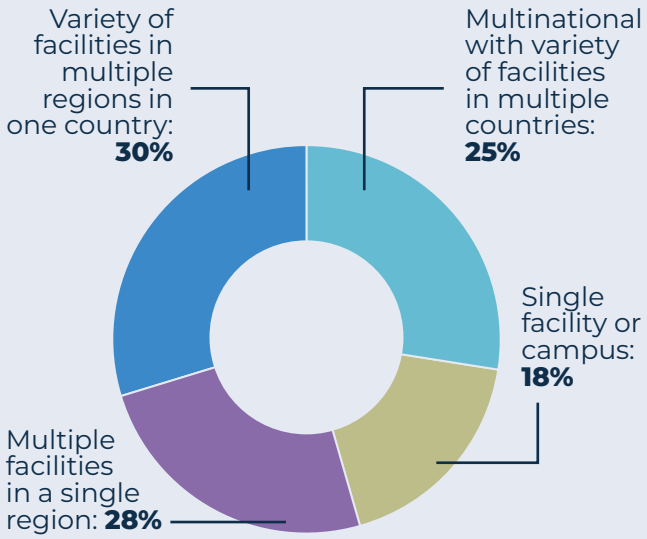
About half of the respondents were from North America (53 percent). Africa, at 13 percent, and Asia at 12 percent were next, followed by Europe at 7 percent; Central America, South America, and Caribbean at 6 percent; Oceania at 5 percent; and the Middle East at 5 percent. Approximately 5 percent selected "other," indicating that no single region encompassed at least 90 percent of the respondent's security scope

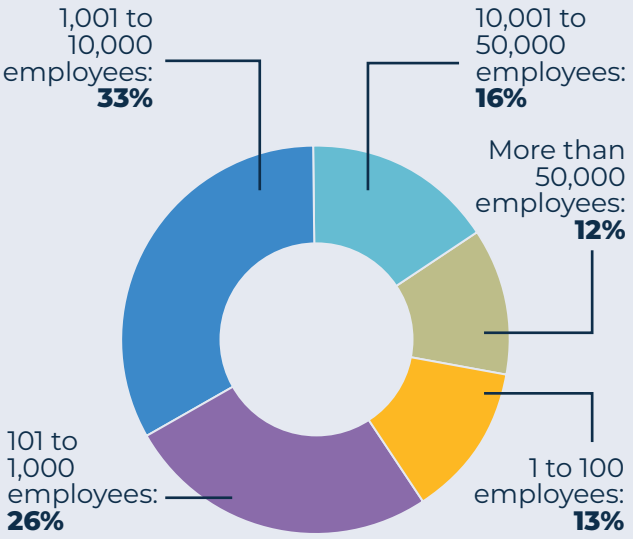
Excluding respondents who said they were either security consultants or security solution providers (which potentially skews size-related demographic data), survey participants were fairly evenly divided by the scope of the facilities for which they worked in security, with the fewest being at organizations with a single facility or single campus of a few facilities (18 percent). Other facility types were all between 25 and 30 percent (see Chart 6).

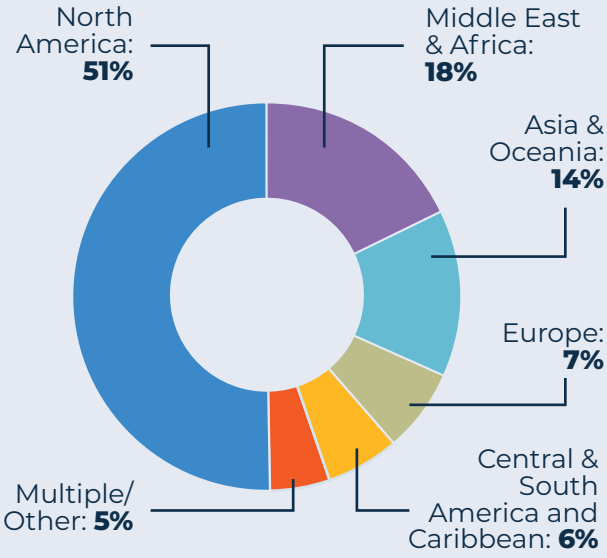
As in previous ASIS research, “Security Services” was the most prominent industry of participants, which is why researchers developed a separate set of questions for consultants and security solution providers. Removing those respondents left two of 22 remaining industries above 10 percent of respondents: manufacturing and banking, finance, or insurance, each of which encompassed 12 percent of respondents.

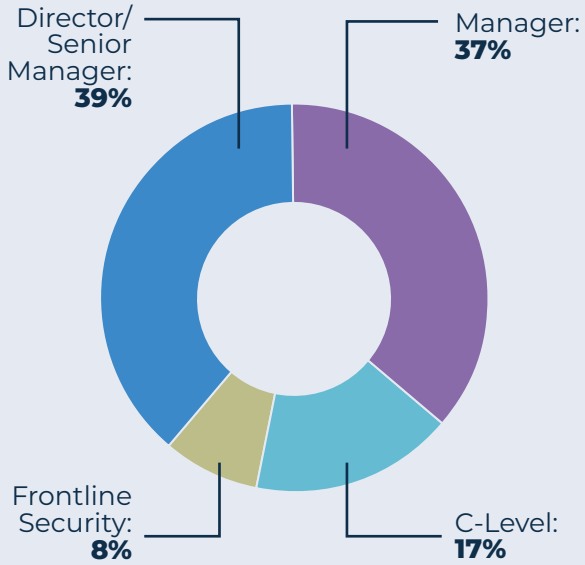
In terms of title, factoring out consultants and those who chose “other,” 133, or 17 percent, were C-suite executives, including chief security officers (CSOs) and chief information security officers (CISOs). The largest contingent were directors or senior managers of security or related positions (39 percent), followed closely by manager level (37 percent). Frontline security personnel comprised 8 percent of participants.

Chart 6: Demographics of Survey Participants







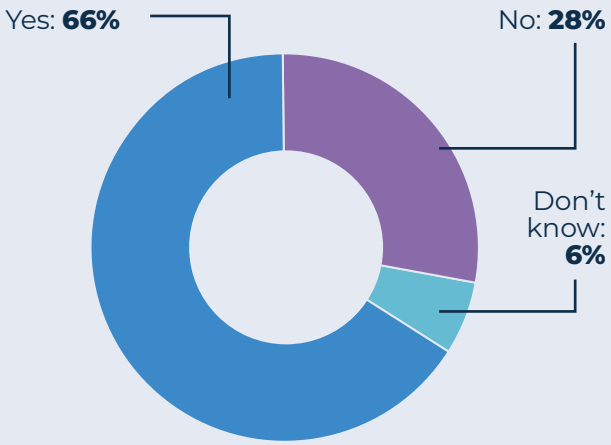


KEY FINDING 1: ACCESS CONTROL SYSTEMS ARE HIGHLY EFFECTIVE

Fully two-thirds of security professionals reported that their access control system is required to meet statutory or other regulatory compliance measures. Of the explicit regulations listed, ISO-9001 (29 percent) was cited most often, followed by OSHA regulations (27 percent), GDPR (18 percent), FIPS201/HSPD12 (17 percent), and department or ministry of defense (16 percent) (see Chart 7). Of course, effective access control systems, defined as both the technology and the policies and procedures designed to control access to a facility or site, are critical in an organization's Duty of Care, which is foundational to all security programs.

In addition 93 percent of respondents reported that access control was an explicit part of a broader risk management or security plan in their organization.

Chart 7: Required by Statute or Regulation to Meet Certain Access Control Standards



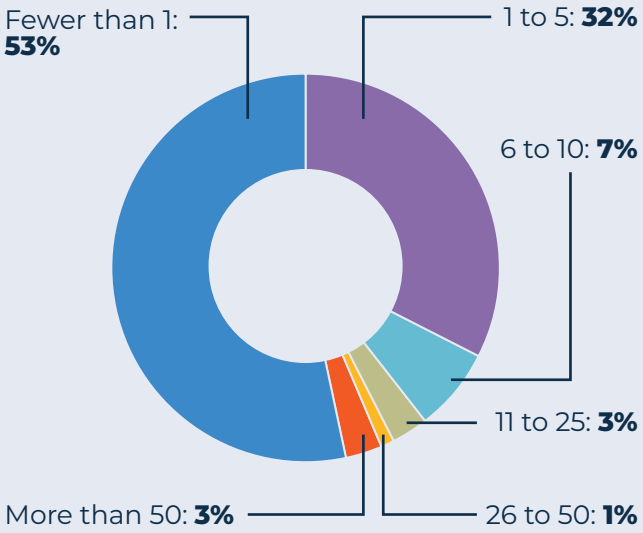
"Access control is primary. It is the beginning of our security process, the umbrella over all of it," said Ross Johnson, CPP, president of Bridgehead Security Consulting. "It helps to ensure that the only people who have access to your people during the workday are people who are authorized, who are approved to be there. It is so necessary to continually revisit the systems and processes you use to keep up with changing threats. The idea of just installing something and checking the box and saying we're done is wrong. My experience is that all security measures begin to decompose after about a month, and so they must be constantly reviewed."

But how effective are the access control systems that they have in place?

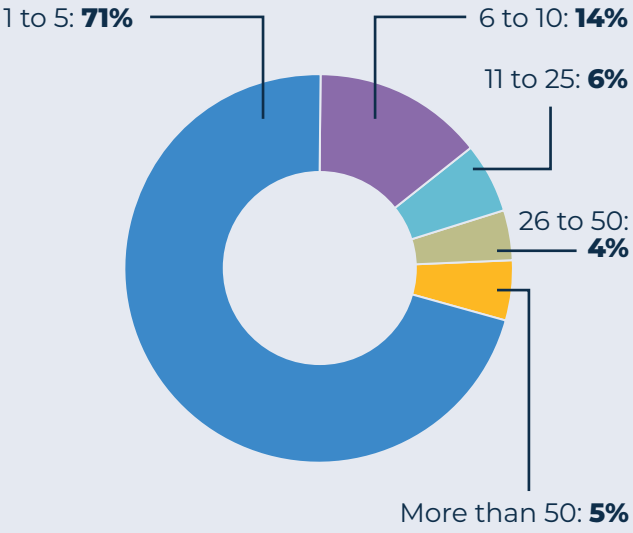
Getting straight at the heart of the matter, the survey asked security professionals about access control incidents in a couple of ways. First, it tried to assess how common incidents occur on a week-by-week basis, asking this specific question: "How many security incidents related to access control or unauthorized physical access do you face per week on average? (An 'incident' is anything that requires security to take extra action to investigate or remediate.)" The choices started with "Fewer than 1" and increased in categories up to "More than 50."

Filtering out those who said they did not know, 85 percent said they average five or fewer incidents per week. Researchers expected to have to crosstab this question with organization size to arrive at workable conclusions. However, there were so few respondents who reported six or more incidents there was no need (see Chart 8), and the only statistically valid reading possible

Chart 8: Access Control Incidents Requiring a Security Response Per Week



Access Control or Unauthorized Physical Access: Serious Incidents Per Year



from the data was that very few access control incidents happen.

The survey also asked "How many critical or serious access control or unauthorized physical access incidents do you face each year?" Researchers left it to participants to decide what constituted a "serious" incident. Still, the results were remarkably consistent with the weekly results: Fully 71 percent said they faced no more than five serious incidents and a total of 85 percent had fewer than 10 incidents. Taken together, the two results show that access control systems are remarkably effective, and this is despite the myriad ways they could be compromised, from technology failure to sabotage to human error.

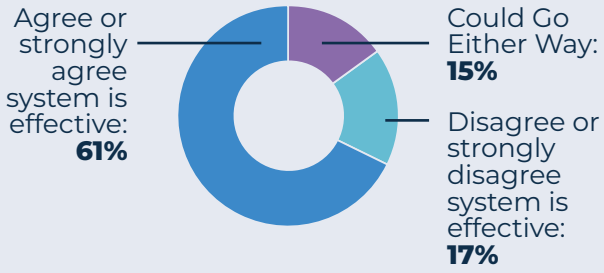
The research gauged security professional attitudes on how effective they thought their access control system was by presenting a series of statements and asking security professionals to rank how strongly they agreed with each statement. While the weighted averages all veered toward the "agree" side, the responses showed there may be plenty of room for improvement in access control systems. For example, to the statement, "I am confident our access control system is highly effective at protecting the organization," 61 percent of security professionals either agreed or strongly agreed. But that means 39 percent either disagreed with the statement or said they could go either way in the rating. (Note: these ratings will be referenced in each of the next sections of the full report to help assess the effectiveness of various technologies and practices.)

In addition, while weekly incident rates were low and major incidents were rare, access control system failures occur regularly.

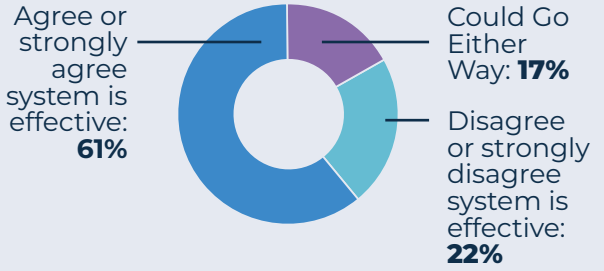
"If you go back to the fundamentals of it, access control is a means to control who is going to come in and who is leaving, and keeping track of it all. One of the issues you will have when approaching it from the security per-

Chart 9: Rate How Strongly You Agree with Each of These Statements

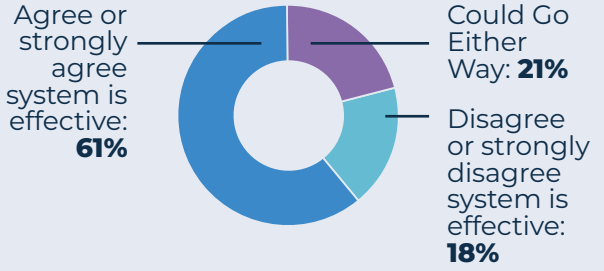
I am confident our access control system meets all necessary requirements for employees.



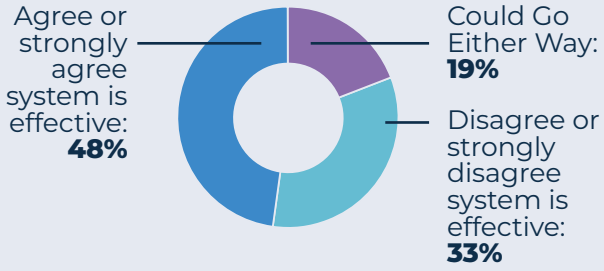
I am confident our access control system meets all necessary requirements for visitor, contractor, and temporary staff management.



I am confident our access control system is highly effective at protecting the organization.



I am confident we deploy state-of-the-art access control technology given the level of control we need.



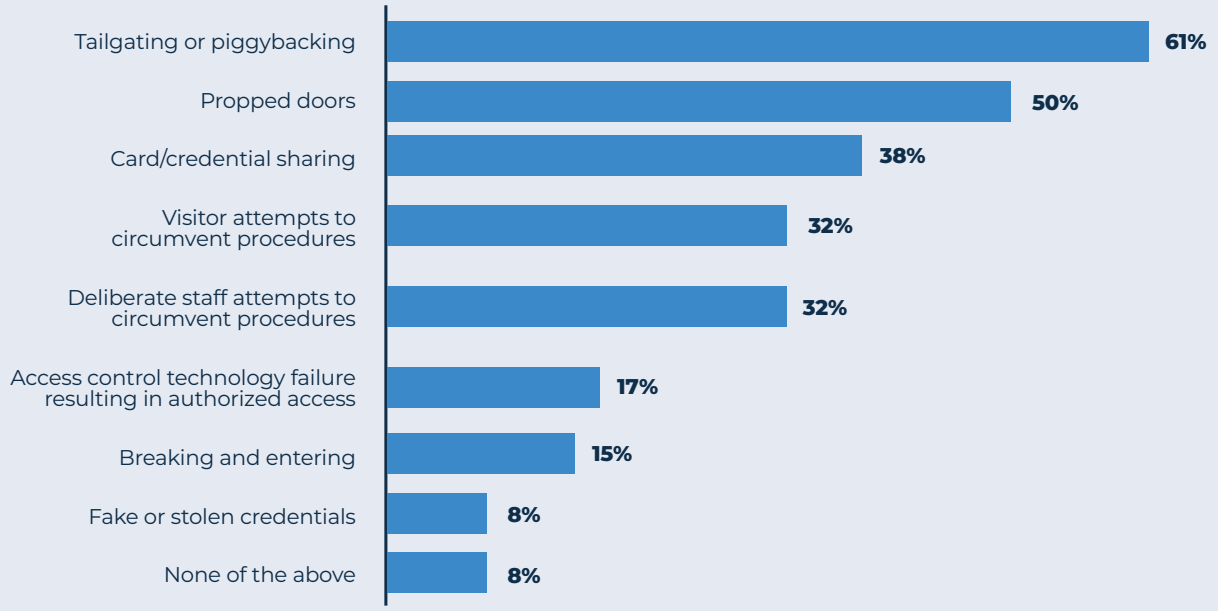
spective is… [staff's] learned behaviors," said Don McInnes, PSP, a physical security and fire alarms specialist. "People can get real used to propping a door open or holding a door open, negating the whole purpose for the access control." McInnes "The people who want to bypass the access control system, usually they don't defeat the security hardware. They take advantage of the people that are utilizing it and are not doing so properly."

The survey listed types of common access control failures and asked security professionals if they had experienced any of them in the previous six months. Only 8 percent had not experienced any of them. Tailgating or piggybacking topped the list, with 61 percent reporting the issue, followed by propped doors, an issue 50 percent faced in the prior six months. Of the incidents listed, fake or stolen credentials (8 percent) and breaking and entering (15 percent) were encountered with less frequency (see Chart 10).

"Key Finding 4: Integrating with Other Systems Is Vital for Access Control Effectiveness" (page 26) documents the close relationship between surveillance and access control. One of the supporting datapoints is that 76 percent of security professionals utilize surveillance to ensure the access management system has not been breached. There is one category that is at least as important as surveillance, if not a little more so: 80 percent of security professionals employed staff security awareness training to ensure access management is not breached (surveillance and security awareness fall within the margin of error of the survey, so they are technically equivalent).

This finding is bolstered by another survey question, which asked about policies and procedures in place: 75 percent said access control policies were emphasized as part of employee orientation and 61 percent said the

Chart 10: Access Control System Failures Experienced in Previous Six Months



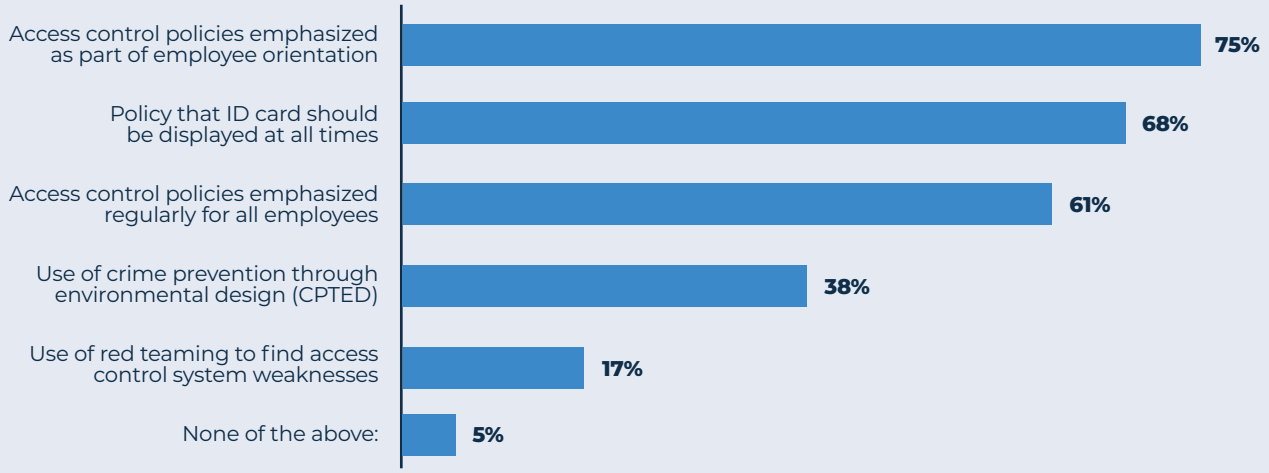
policies were reinforced with staff regularly. In fact, the latter policy—regularly reinforcing access control policies with staff—correlates to how effective security professionals think their access control system is: 70 percent who have the policy agree or strongly agree that their access control system is highly effective at protecting the organization versus 61 percent of all security professionals.

Stephen W. Di Rito, vice president, chief security officer of HealthPartners based out of Minneapolis, Minnesota, said it is important to start with a detailed, written policy detailing important security policies and procedures—he calls it a standard. "Of course, those are the kinds of documents that nobody reads, but you have it there and ready so you can refer to it and you are consistent in your approach, and people who really have questions or concerns can access it."

Dealing with physicians, nurses, and other healthcare professionals, time is at a premium. Some topics or issues will require a 30- or 60-minute meeting—you can't eliminate that entirely. But Di Rito augments his security messaging with a specific approach. "We call it 'Secure59' because it takes less than a minute. Take the issue of tailgating, for many organizations, it's a big problem, and it's a problem for us. To reinforce our security messaging, we created a short video, less than a minute, that describes tailgating, tells them our policy, and describes what can happen when people allow others in without the proper clearance to access a more secure space. The video series has been highly effective."

There is one technique to dramatically increase the effectiveness of access control systems that relatively few organizations take advantage of: Only 17 percent of respondents reported that they used red teaming to test the effectiveness of their access control system. Red-teaming is the systematic approach to actively try to find vulnerabilities in system. Security profession-

Chart 11: Access Control Policies and Procedures Used by Organization

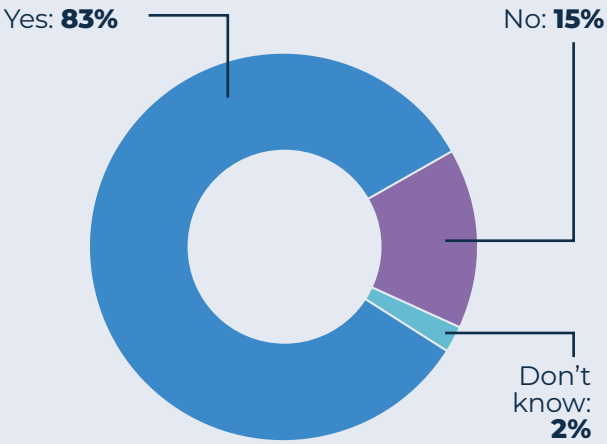


als that use red-teaming to test their access control systems have much higher confidence in their systems: 82 percent agree or strongly agree that their access control system is effective, again compared to 61 percent of all security professionals.

Any number of security consultants are highly trained at red teaming and can provide security professionals with a lot of data that will help them improve their access control systems. Such ammunition can help convince reluctant decision makers to carefully consider upgrade recommendations. However, a more informal red-teaming approach can also be highly effective.

"Have you ever heard anybody say, 'Oh, I know how to get around that security system.'? What I realized is, that's like a near-miss in the security and safety world," said from Bridgehead Security Consulting. "They're telling you something. So in the future, what we need to do is get people to put that in writing and send it in, or we need to make notes. They're telling you the weaknesses you have in your physical protection systems."

Chart 12: Employ Varying Level of Access Control Depending on the Risk Profile of the Asset Being Protected



The following four charts depict access control system benchmarks for organizations, some of which were referenced in the preceding discussion, and some of which are new information. The first one depicts the full policies and procedures benchmarks that were just discussed.

Chart 13: Methods Used to Detect Access Control Breaches

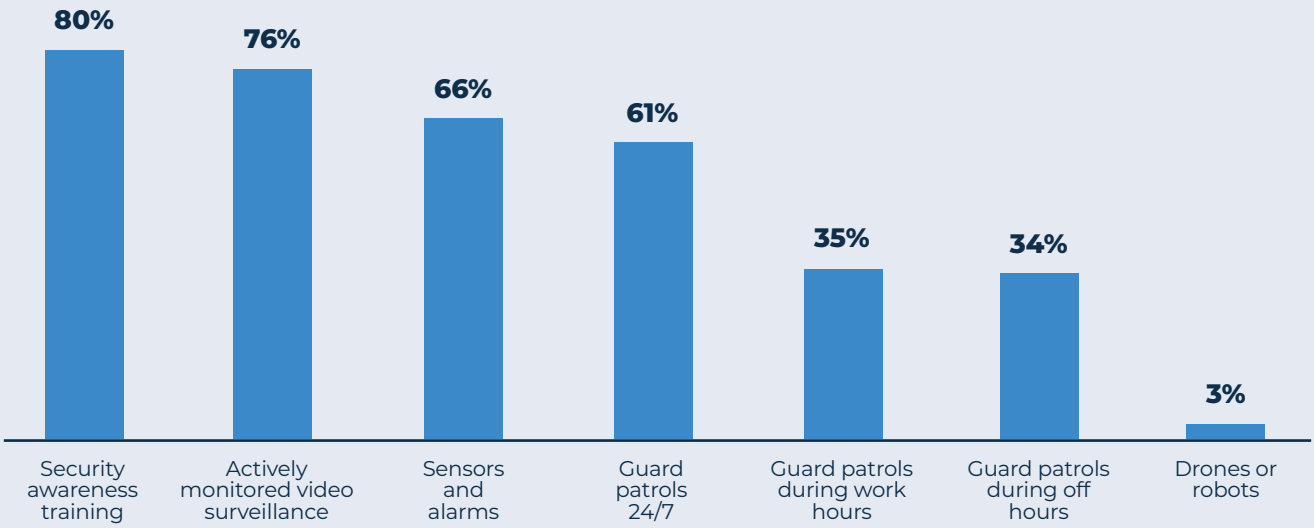
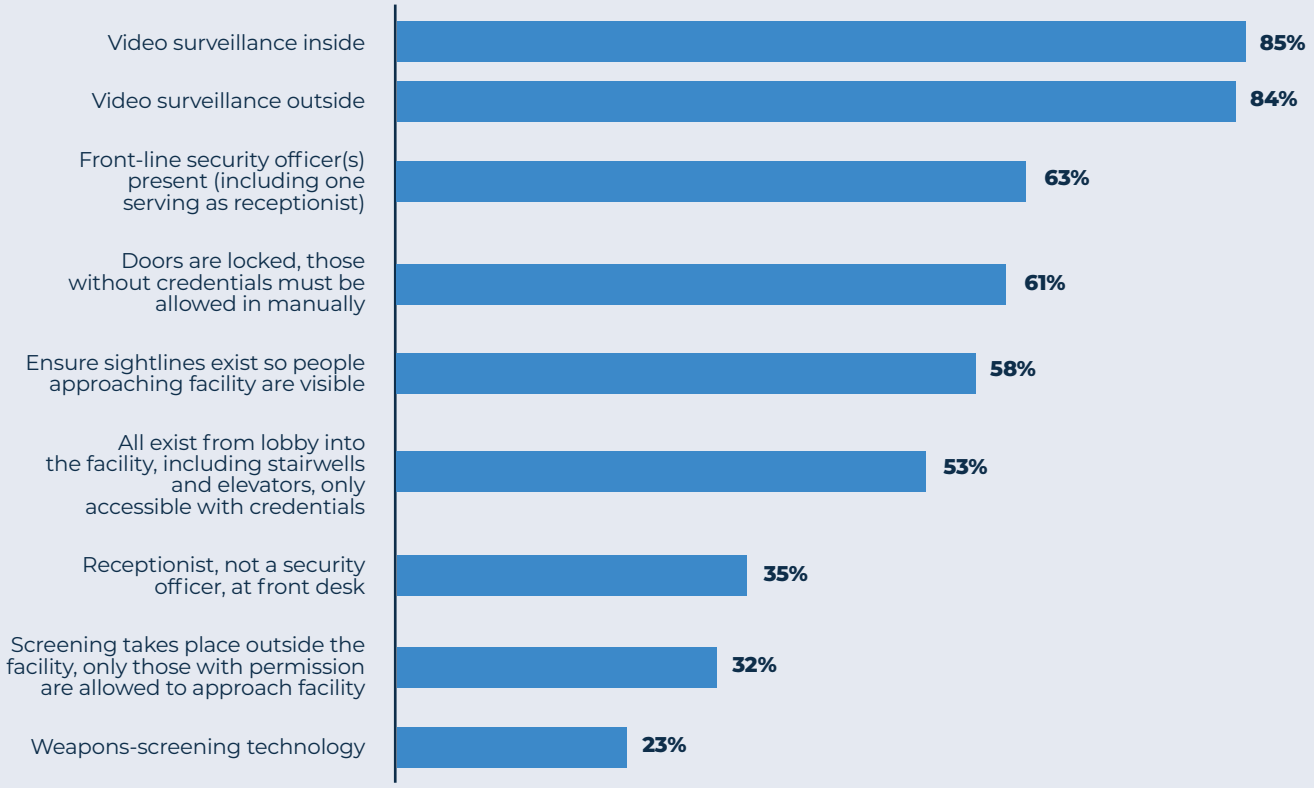


Chart 14: Security Measures in Place at Primary Entrances



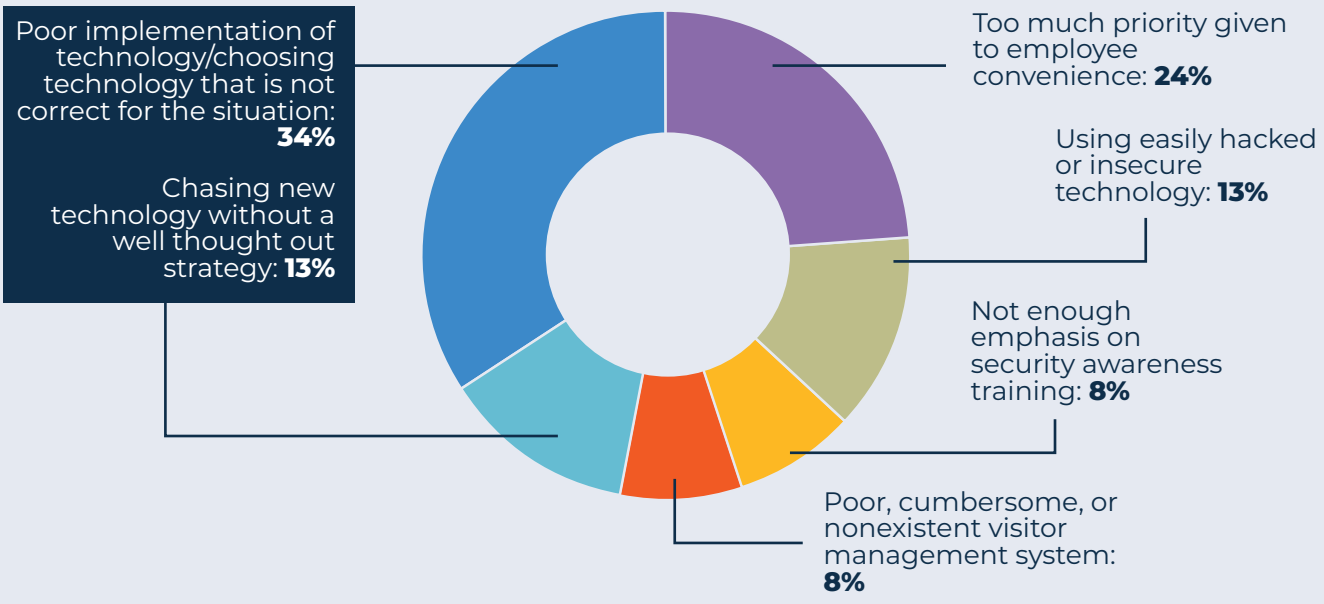
KEY FINDING 2: COMPANIES ARE SHIFTING TO MORE SECURE TECHNOLOGY

One of the reasons the researchers have emphasized several times in this report that the access control system is defined as both technology and policies is because the term itself—access control system—is often used interchangeably with access control technology. Thinking of the word system in this way is, in fact a trap. The preceding section highlighted many ways that the policies and procedures part of the system are every bit as important as the technology.

The consultants, in their survey, warn against the demons of chasing technology. They were given six possible access control failures and asked which they see the most in their practice. Nearly half chose one of two choices related to improper deployment of technology (see Chart 15).

While it is important to keep the technology side of the access control system in the proper perspective, technology is, of course, a critical component of effective access control. Most access control systems long ago abandoned lock and key as a primary method for locking down a facility or location, replacing them with electronic means of credentialing and authentication. The survey asked security professionals to select all the types of access control technology they employed and provided 12 methods to choose from (see Chart 16).

Chart 15: Which Access Control Concerns or Failures Do Consultants See Most



Several of the types are known to have security deficiencies. Access control solutions using 125 kHz low-frequency proximity cards became ubiquitous when the previous king of access card technology, Wiegand magstripe cards, was shown to be easily bypassed or the cards spoofed. Unfortunately, the low-frequency proximity cards did not wear the crown for very long. After several years of the low-frequency cards building market share and becoming the primary credential, it, too, soon proved vulnerable. Anyone who could purchase $100 worth of equipment, do 20 minutes of internet research, and put forth a little reconnaissance effort could easily gain entrance.

The good news is, use of the least secure access control technologies is declining. A 2019 study from ASIS showed that 51 percent of respondents used 125 kHz low-frequency proximity cards. That number declined to 22 percent in this study. Likewise use of magstripes fell from 26 percent to 7 percent.

Researchers categorized the list of credentials into three categories, acknowledging that this categorization is a generalization only, and will not cover all use cases. The breakdown is as follows:

Security Level	Credential Type
Low	Keypad; Wiegand; Magstripe; Barcode or QR Code; 125 kHz low-frequency prox
Medium	RFID prox card; Smart RFID card
High	Mobile Device; Biometric (all types); Multifactor

Because many organizations will employ multiple types of access credentials depending on their analysis of their needs, researchers analyzed all survey responses and recategorized them. Those who only used credential types with a low

Chart 16: Access Control Credentialing Technology in Use

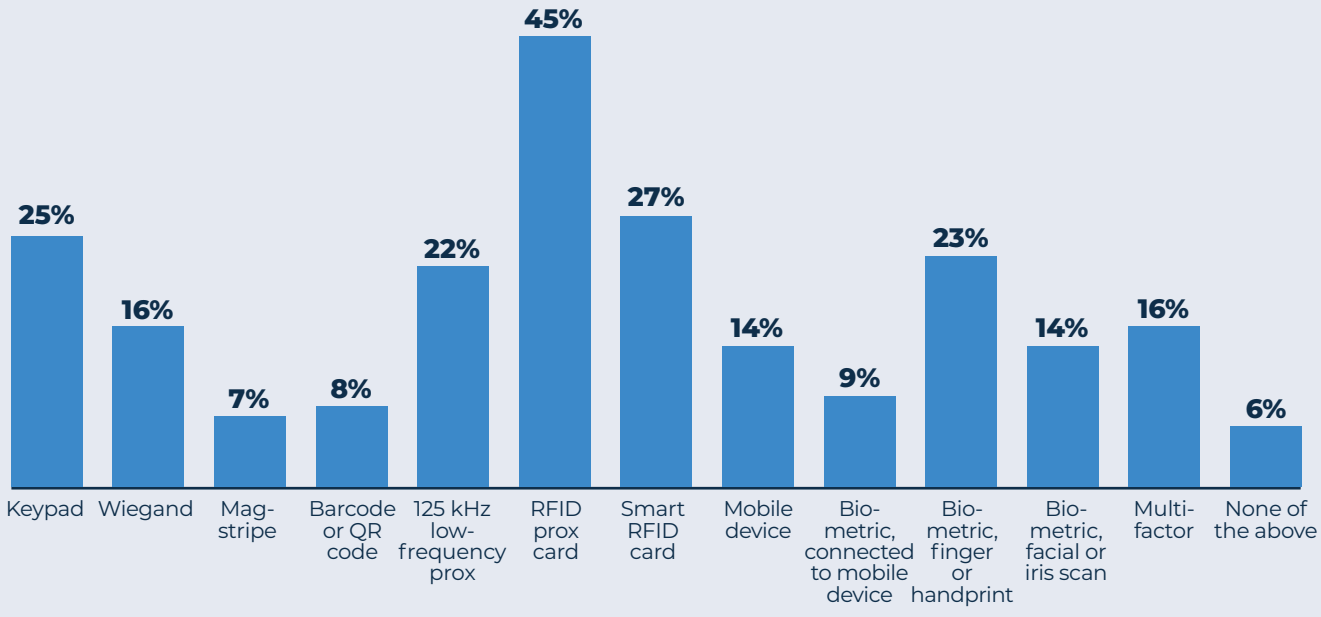
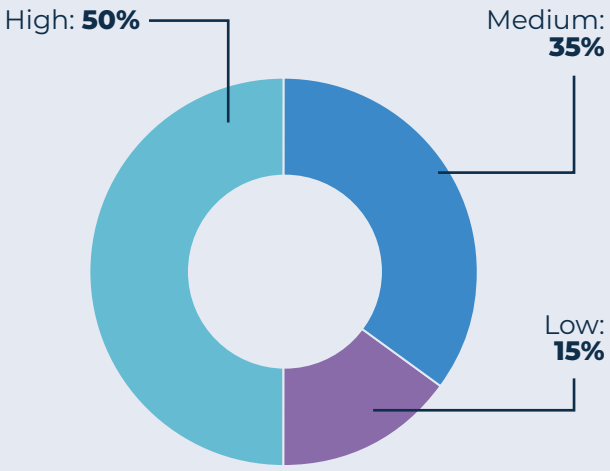


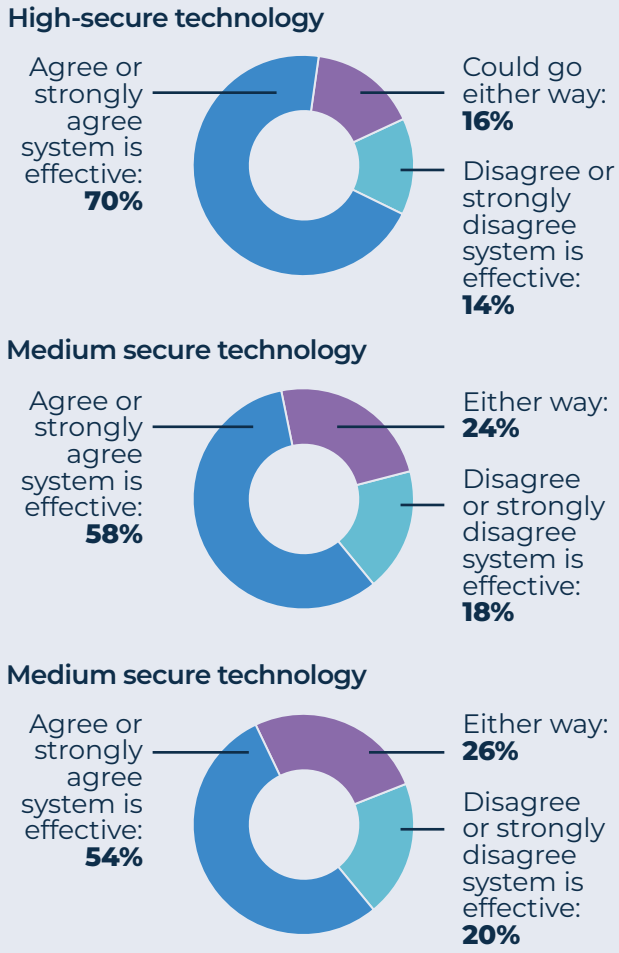
Chart 17: Percent Who Rely on Low-Security Technology vs. Have Higher-Security-Level Technology in Use



security level fell into the low category. Those who used medium security level credentials—whether only using medium level methods or a combination of medium and low security levels—were reclassified as medium. Similarly, those using high security level credentials fell into the high category (see Chart 17).

Not surprisingly, security professionals who deploy technology classified as a higher level of security are more confident in their overall access control system. The survey asked participants to rate how strongly the agreed with the statement "I am confident our access control system is highly effective at protecting the organization," with 1 equaling "strongly disagree," a 3 equaling "could go either way," and a 5 equaling "strongly agree." The weighted average of high security technology respondents was 3.79, for medium security technology, it was 3.52, and for low security technology, it was 3.40. The difference is easier to see when comparing those who chose 4 or 5 compared to those who didn't (see Chart 18).

Chart 18: Security Level of Technology Compared to Feelings of Effectiveness of the System



The survey asked respondents about their access technology upgrade plans: 13 percent had upgraded in the past 12 months; nearly half (47 percent) were either in the middle of an upgrade or had firm plans to upgrade within the next two years; 15 percent said upgrade plans were more than two years off; and one quarter said they had no upgrade plans.

Of those who had recently upgraded or planned to upgrade in the next two years, by far the most

important feature desired as part of the upgrade was integration with other systems: 61 percent. Upgrading to smart RFID cards and readers was second, with 47 percent. Other selections, including deploying multifactor authentication or deploying technology utilizing mobile device credentials, hovered between 36 and 39 percent (see Chart 23 in the "Key Finding 4: Integrating with Other Systems Is Vital for Access Control Effectiveness" section on page 26).

Of course not all upgrades are for everybody. Di Rito, with HealthPartners in Minneapolis, is in the middle of a massive upgrade of the entire physical security technology structure to get multiple facilities all using the same platform. One thing he said he hopes to avoid is mobile credentials, for a very specific reason:

"I have not had people asking about mobile credentials yet, but I anticipate it's coming, and I want to try to stay away from that if I can," he said. "Coming from the corporate world where it was often a challenge to get employees to wear identification badges, in healthcare, that is not the case. Staff is used to displaying badges at all times. I think mobile credentials help people get on the path of not wearing a badge, and I want them to have that ID badge on."

In addition to the technology solutions deployed, an effective access control system means capturing and making use of data. Access control technology can create massive amounts of data, which can be mined and used to increase the effectiveness of the system as well as for other business objectives.

In Johnson's experience, which includes work in some highly regulated industries, priority was given to data and metrics that concerned the regulations the company had to meet.

"Things like door alarms were definitely recorded and reported because it was a regulatory requirement that we do so. We use log data and video, primarily for investigations, but those anomalies that related to anything in the regulations, those took priority to ensure we stayed in compliance."

Speaking of door alarms, that's the bugaboo of Di Rito at his hospitals and healthcare facilities. "The volume of alarms was overwhelming the operators, to the point that you just start ignoring the alarms. We were getting 4.7 million alarms a month, so that's a system that's never really been touched. We're using data to identify the top 10 alarms, working to address those, and then going to the next 10. Our hope is to knock it down to 25,000 to 50,000, which I think we'll be able to do. One door was giving us 30,000 alarms a month, and so that's a door malfunctioning. We can eliminate those alarms by getting maintenance to address the issue."

From there, Di Rito will categorize the alarms to make them more manageable and increase the effectiveness of his security operations.

The survey asked security professionals what access control data they used. Just under 10 percent said they did not use any access control data. Video recordings of access points led the way, with 62 percent. Alarms or related reports (51 percent), time and attendance (48 percent), and access log anomalies identified manually (42 percent) were also prevalent. Fewer used data to measure convenience factors, such as visitor processing times (20 percent) or throughput or queuing times (9 percent). Use of machine learning or AI to analysis access logs, as opposed to finding issues manually, was also only sparsely deployed (10 percent).

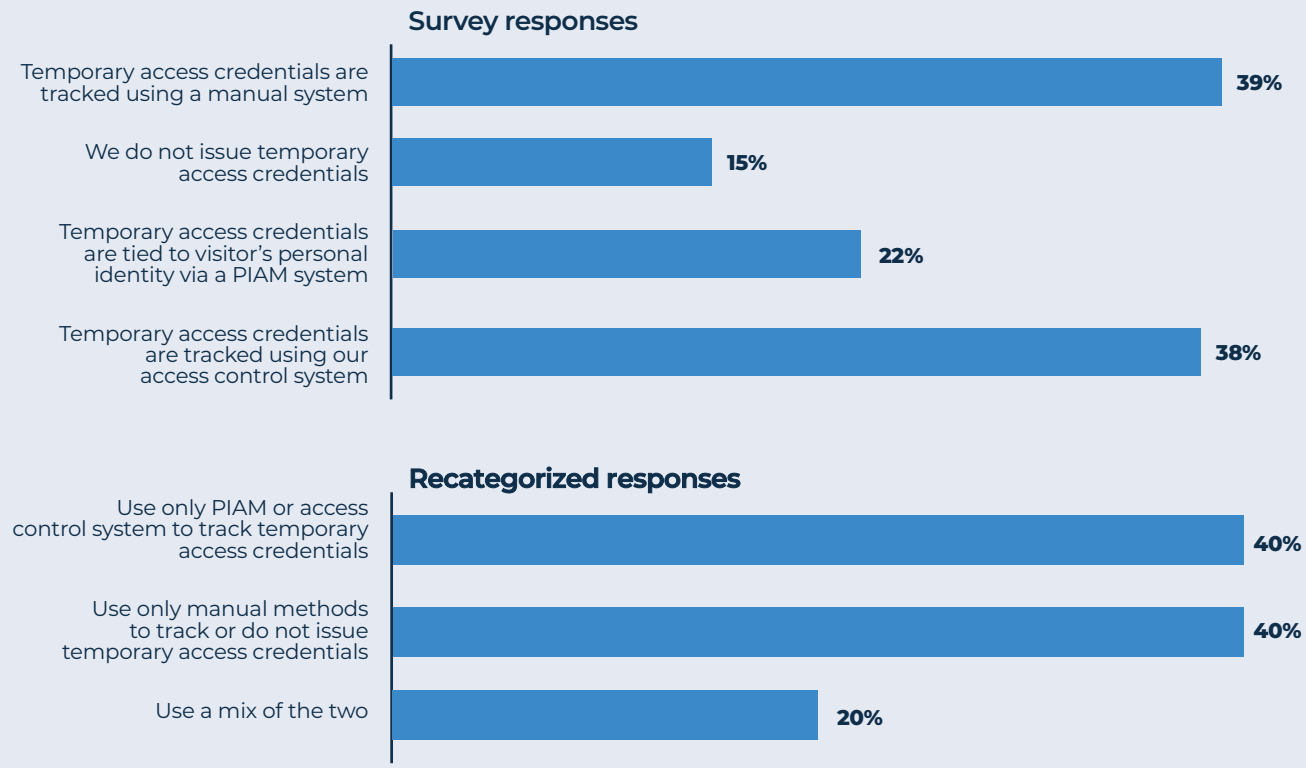
KEY FINDING 3: VISITOR MANAGEMENT PLAYS A CRITICAL ROLE

The number of access control variables related to visitor management are numerous. Organizations must account for such varied situations as a customer coming to a facility for a one-hour meeting to regular contractors coming multiple times per week to contractors or temporary employees with durations that can span days or weeks or even months. The survey asked several questions about the technology used to support visitor management as well as policies in place and effectiveness measures.

On the technology question, 39 percent reported that they used a manual system, such as pen and paper or a spreadsheet, to keep track of temporary credentials issued to visitors; 15 percent said they did not issue temporary credentials. Participants could choose any of the options that applied to their situation, and so the percentages added up to more than 100 percent. One possible explanation is that organizations have different visitor management practices at different sites. The top half of Chart 19 presents the overall data while the lower half presents recategorized results.

This result showed that, assuming the explanation in the preceding paragraph is correct, 40 percent of organizations use either a physical identity and access management system or a different access control technology to track temporary credentials at all of their sites, 40 percent use only a manual system or do not issue temporary credentials, and 20 percent use

Chart 19: Characteristics of Temporary Access Credentialing System



a mix of manual (or do not issue) and digital systems to track temporary credentials.

In addition, 31 percent of security professionals reported that not all visitors, contractors, or temporary workers received access credentials, mostly dependent on access needs; 23 percent said whether or not temporary credentials were issued depended on the length of the visit.

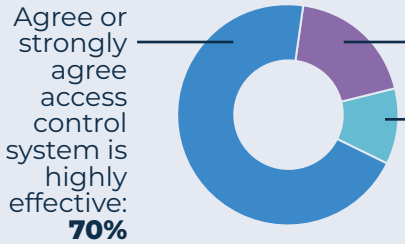
Those who reported using a manual system or that they did not issue temporary credentials were asked why they did not use a dedicated digital system to track temporary access credentials. Forty-one percent said it was part of an upgrade plan that had not been installed yet. Each of the other options provided in the survey were cited by around one-quarter of participants, including “systems are too expensive” (28 percent), "not enough visitor traffic to warrant a dedicated system" (29 percent), and "risk assessment has not identified this is a priority" (25 percent).

It also turns out that security professionals who report that they use PIAM or other access control technology to digitally track temporary credentials are more confident that their overall access control system is effective than those who do not issue temporary credentials or who track them manually. Nearly 20 percent more of the former group either agree or strongly agree with the statement "I am confident our access control system is highly effective at protecting the organization." (See Chart 20.)

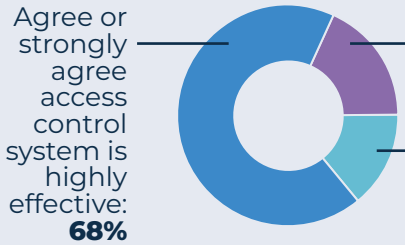
The survey also asked about visitor policies in place. Requiring visitors to show identification is a common policy, with 69 percent of security professionals saying their organization had the policy. Less ubiquitous, but still heavily used, 37 percent said all visitors must be known in advance and prescreened by security (see Chart 21). Several of the policies also have statistically significant correlations to how effective the security professional thinks the overall access

Chart 20: Effectiveness of Overall Access Management System by Temporary Credential Method

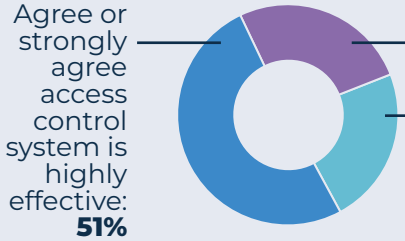
Use PIAM to track temporary credentials



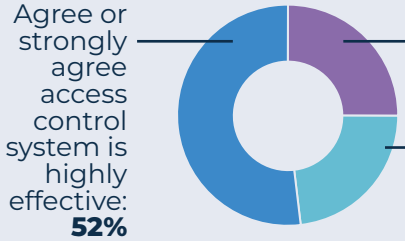
Use access control technology to track temporary credentials



Use manual method to track temporary credentials



Do not issue temporary credentials



control system is. Compared to a baseline of 61 percent of all survey participants who said they were confident their system protects the organization the following policies boost the percent who are confident: visitors showing a government identification (68 percent), restricting access to offices or rooms near the entrance (70 percent), visitor prescreening by security (68 percent), and visitors must be escorted (69 percent). The other policies also boosted confidence, though by smaller amounts that may not be statistically significant.

The survey also asked participants if their access control system was integrated with a visitor management system: 42 percent said they did. Use of such a system is also strongly associated with being confident in the overall effectiveness of the access control system (see Chart 22).

Chart 21: Visitor Management Policies and Practices

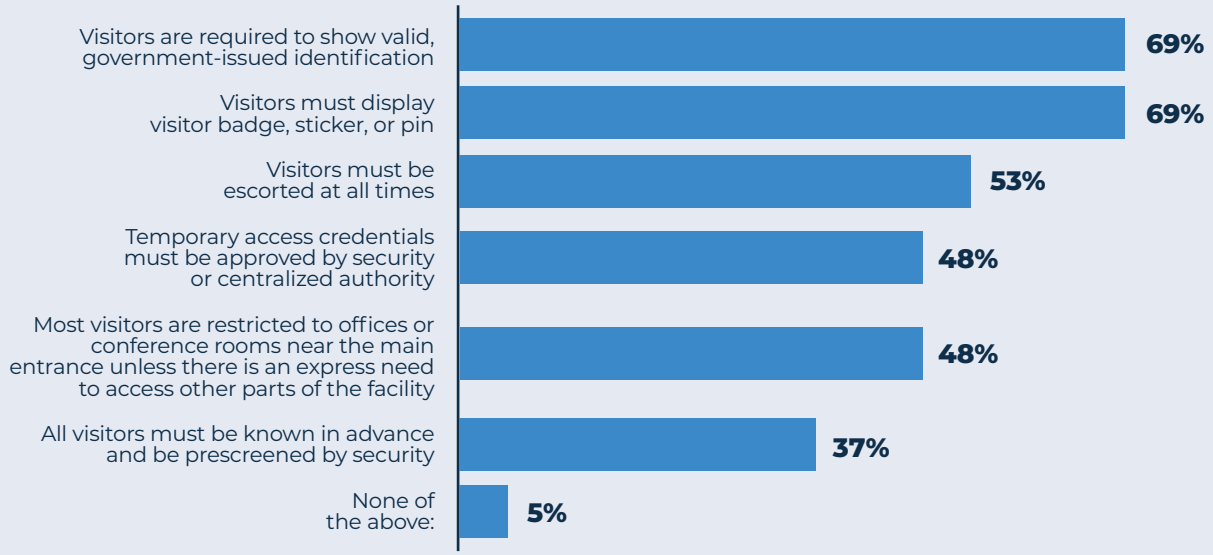
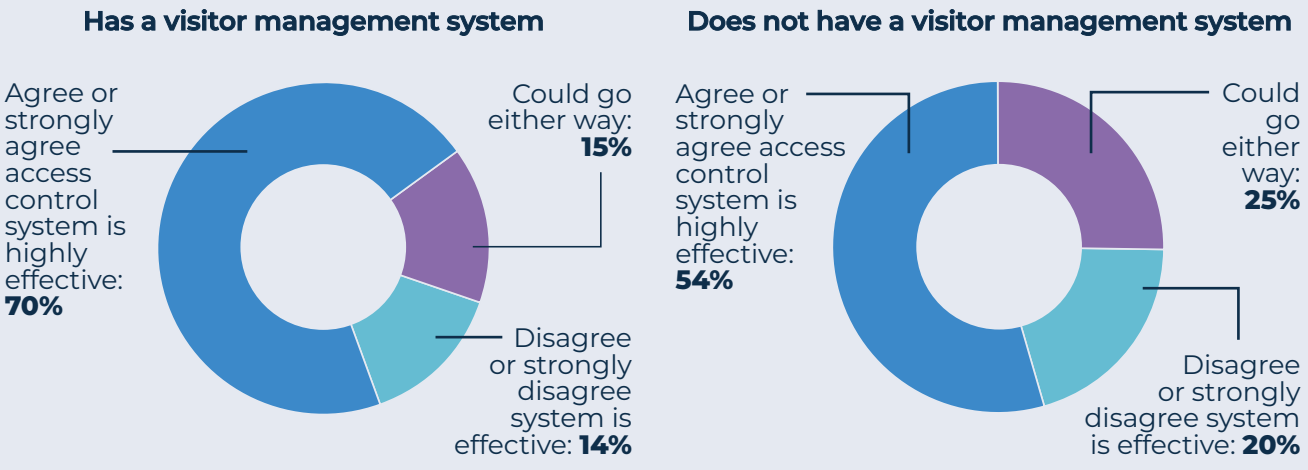


Chart 22: Visitor Management System Impact on Effectiveness of Overall Access Management System



"I would love to have a visitor management system," said Parnell Lea, director, security and life safety at Brookfield Properties, which manages high-rise office buildings and is based out of Calgary, Alberta. "The problem is our buildings are open with numerous clients in each building. We would not use it for people visiting our clients, that would not be a workable situation. But a visitor management system would sure make working with contractors easier. We have our workaround systems, a paper process. We've had discussions with a couple of vendors, because we'd sure like to eliminate the manual recording, but so far, we haven't found a solution that meets our needs that would be worth it."

One benchmark important to many organizations is how long it takes to process visitors into a site. Taking out those who said they did not know, the vast majority reported that processing visitors took between one and five minutes (62 percent). One in ten said it took between 6 and 15 minutes, and 14 percent processed visitors in less than a minute. Seven percent said it varied greatly depending on circumstances, leaving 2 percent who said the process took longer than 15 minutes.

Underscoring the importance of getting the visitor management part of an access control system right, the survey ended with an open-ended question asking security professionals what they would change about their access control system if they could. The word "visitor" was the fourth most-used word behind "integration," "technology," and "improve." A sampling of those comments (some of them slightly edited for clarity):

What Security Professionals Would Change About Their Access Control System: Visitor Management Responses

"Employ a digital dedicated visitor management system."

"E-gate pass instead of a paper-gate pass for visitors."

"The time wasted during visitor registration."

"Link visitor management with access control system and integrate video."

"Not necessarily change the access management system, but add visitor management solution."

"If cost wasn't an obstacle, I would make our visitor ID/sign-in process less reliant on paper and pencil."

"Advanced notice of all planned visitors."

"Limit visitor access on a greater portion of campus."

"Our role as a public institution doesn't have to mean we make security compromises—it should mean the opposite and we should have stronger mandates for visitor control campuswide."

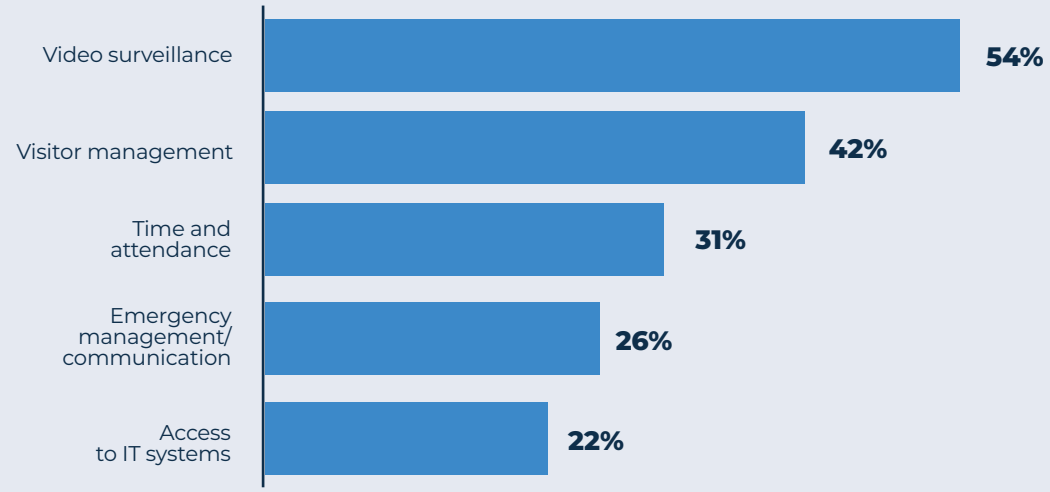
KEY FINDING 4: INTEGRATING WITH OTHER SYSTEMS IS VITAL FOR ACCESS CONTROL EFFECTIVENESS

The benefits of linking surveillance systems and access control is both obvious and very much in practice. Asked to select from a list of nine security features—from cameras to receptionists to locked doors—that their company employs at primary entrances, video surveillance inside (85 percent) and outside (84 percent) were by far the most used (see Chart 14 on page 17). In addition, when asked how they ensure their access control systems had not been breached, 76 percent of security professionals said they actively monitored video surveillance (see Chart 13 on page 17).

The survey asked which technologies were integrated with access control technology, and once again the video surveillance system topped the list, with 54 percent reporting that video and access control technology were integrated (see Chart 23). Other systems often tied to access control technology include visitor management (42 percent) and time and attendance software (31 percent). Emergency management systems and tying access control credentials into logical IT systems access are less frequent integrations.

"We're trying to get our CCTV and security systems on to one platform," said Lea from Brookfield Properties. "We'd like to be able to operate everything off of one screen. We have one property that operates that way now, and the guards absolutely love it. They find investigating and dealing with issues so much better. It works like a dream for them."

Chart 23: Technology Systems that Are Integrated with Access Control Technology



At the same time, simplicity is important to Lea. "A lot of guards come in with only basic knowledge on computers, so we're teaching them, essentially, to use computers. If the system's too complicated, it really stresses them out, and they have a hard time managing it. So what I've found over the years is these systems add so many features, but we barely use any of them, because we have to keep it simplified."

In addition, survey participants were given the opportunity to write in other systems that access control technology is integrated with. A total of 32 people added a response (including one whose access control was tied to a breathalyzer!). The two most widely mentioned were tying access controls into an alarm monitoring system and into a wider human resources system that is broader than simply time and attendance. Payment or transaction systems were also mentioned.

In the consultant's survey, security consultants were asked to rank the importance of seven different technological innovations related to access control. Given a 10-point scale, the consultants gave very few rankings below a five, or a "medium level of importance." So while everything scored highly, "access control integration with surveillance system" made top marks, averaging an 8.63 (with 40 percent of respondents ranking it a nine or a ten). The next highest average ranking was 7.99, given to "linking access controls to critical systems such as IT access." This compared to an average score of 7.85 for "using multifactor authentication for access control," and a 6.48 for "artificial intelligence or machine learning analysis of access control data." Again, all the innovations scored highly, but the two on integrations scored the highest.

The previous section on visitor management explains that an integration between a visitor management system and access control technology had a positive relationship with overall effectiveness of the access control system. Similarly, integrating a video surveillance system with an access control system resulted in a significant increase in the number of security professionals who were confident their access control system was highly effective at protecting the organization—to 70 percent, versus 61 percent of the full survey.

OTHER FINDINGS, BENCHMARKS, AND FINAL THOUGHTS

There were several other findings that did not contribute meaningfully to one of the key findings, but are nevertheless interesting as benchmarks if nothing else. One of them was how many organizations had access control technology that could track both entry and exit so that at any given point in time, who was in a facility was reasonably known. This is an important emergency management consideration, and can be useful information when conducting investigations.

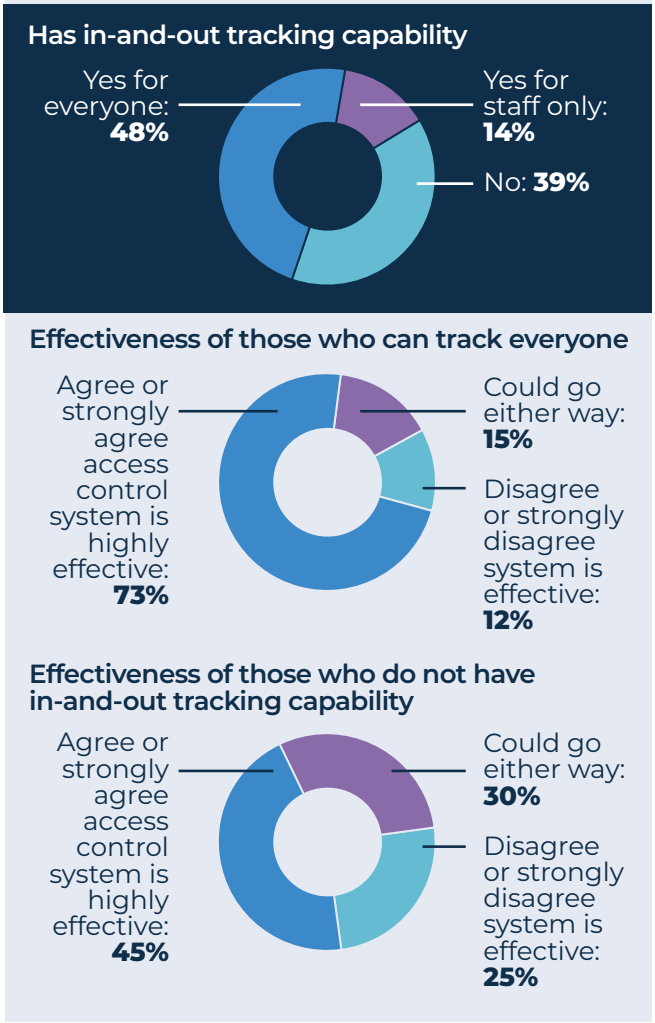
Overall, leaving out the small number who said they did not know, 47 percent of security professionals said they could track all the people in a facility, 14 percent could track all staff, and 39 percent said they did not have this capability.

In addition, just as with other advanced applications, such as integration with video surveillance or visitor management applications, being able to track in-and-out access contributes to the belief that the access control system overall is highly effective at protecting the organization (see Chart 24).

Chart 14 on page 17 depicts security measures in place at primary entrances. The survey also asked about other entrances that were regularly used. Nearly 7 in 10 had nonprimary entrances that were used regularly (69 percent). The survey asked what measures were in place at these secondary entrances, and the results largely mirrored primary entrances (though the survey did not ask about receptionists at these locations). (See Chart 25.)

One notable finding that will bear watching is the low adoption of certain advanced technologies. In what will be an interesting benchmark to compare to future developments, 14 percent of security professionals said they used facial recognition or iris scanning biometric technology as part of their access control system.

Chart 24: Ability to Track In-and-Out Access and Its Effect on Effectiveness



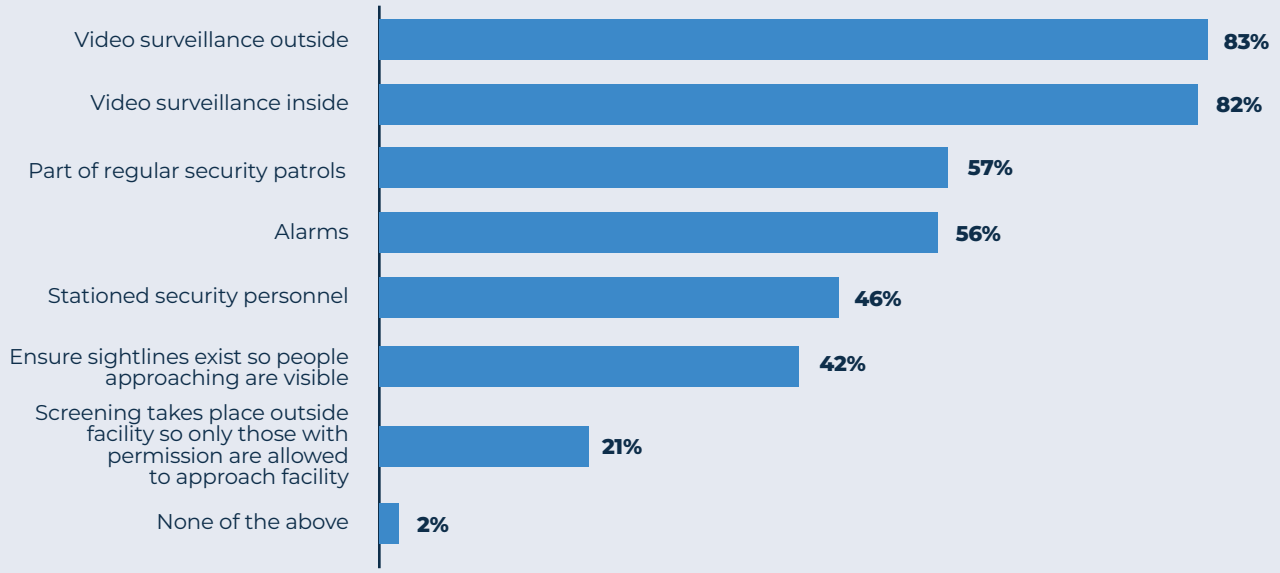
With the advances made in facial recognition technology and the high use of video camera systems, facial recognition could rapidly expand in use the way Wiegand technology replaced keys and locks and the way proximity cards replaced Wiegand. The technology is already widely used in the air travel space. Some countries, such as China, have seen an explosion of facial recognition use, to include gaining access to retail stores. Some sports and entertainment venues have begun experimenting with using facial recognition to replace event tickets. And, of course, the technology introduces a host of privacy and discrimination issues that governments and companies will have to parse out in the months and years to come.

"Technology is eventually going to save us when it comes to people circumventing access control measures," said Johnson. "Facial recognition technology is touchless, as you approach the door of your building, it sees you, it sees that you're allowed to be there, and it will open the door. If it sees someone else there, someone tailgating, an alarm goes off and the doors seal. Facial recognition will also simplify knowing exactly who is in the building at all times."

Less in line for an explosion of activity, but budding technologies nonetheless, use of drones or robots to aid access control systems—including searching for individuals who have gained unauthorized access—was at a paltry 3 percent.

"We're looking at robots for our atriums and food court areas," Lea said of the high rises he manages. "Those are places where most of our activity happens, and if we can get extra eyes for the guys in the control room to watch what's happening, that can be important. We're also looking at robots in parking areas. The problem so far is the robots are not equipped with LIDAR, so they can't detect vehicles pulling out of spaces. So these are things we're looking at, but right now they're either not quite right or cost prohibitive."

Chart 25: Security Measures Taken at Secondary Entrances Other than Card or Biometric Readers



Likewise, 42 percent said they manually scoured access logs for anomalies while only 10 percent said they used artificial intelligence or machine learning to do the job. In both cases, technology could be used to free security's time to focus on higher value endeavors.

Among access control factors that the study did not cover well or that arose during analysis include two areas researchers want to call out.

First, several interviews emphasized the role of access control in a layered security environment. At its core, a layered security environment incorporates the five Ds: deter, detect, deny, delay, and defend.

"What your intrusion detection and surveillance and barriers do is make sure that the only people that get in are the ones that go through your access control system, where you can filter out the people who are not allowed to be there," said Johnson. "The problem is the way it works is you need the earliest possible detection of an intruder, the earliest possible assessment that they are a threat and then you have to delay them until law enforcement or a response force capable of handling the situation shows up. That's the only way it works. What we're seeing is a lot of detection and no assessment or you'll see detection and assessment being far too close to the middle. It needs to be out as far as it can be. And what we also see is not anywhere near enough delay. …The big takeaway for the access control system is it's part of your physical protection system, and it needs to be tested as part of that system."

This study examined the defend part, and perhaps a little of the detect part. Future studies could examine the role access control systems might play in deterring unwanted activity, however, the systems absolutely have a role in delaying perpetuators, and studying how they can effectively contribute to the delay part of the layered security environment would be worthwhile.

Speaking of effectiveness, the primary gauge used to study effectiveness in this study was the question asking security professionals to rate how confident they were that their access control system protected the organization. Researchers actually developed several questions designed to measure effectiveness, including ones that were more direct measure of effectiveness than an opinion. The questions that asked about the frequency of access control incidents, in addition to being good benchmark metrics, were intended to be used as effectiveness measures.

However, it turns out access control systems are too effective overall for these two broad questions to be useful: there were too few security professionals who experienced access control incidents for the questions to be statistically significant measures of effectiveness, beyond just showing that overall, the systems were highly effective.

"If your access control system is working, then I can see why it was one incident or less per week for most companies," Johnson said. "That's why you have access control."

In fact, there was even a third question asking about incidents (you can see the full survey with summary results in the appendix), but the results were so unusual that no useful information could be obtained. The survey asked how many of those weekly access control incidents that occurred were false alarms. The answers yielded an inversion of the standard Bell Curve—40 percent were 10 percent or less and 35 percent were 90 percent more, with the rest smattered in the middle. With such extreme polarization of responses, the researchers decided the question was not clear and decided not to use it in the analysis.

A future study could ask more detailed questions about access control incidents and failures and derive better effectiveness measures.

Overall, the state of access control in organizations is strong. Most organizations have put some of the most meaningful best practices into place—including having access control be part of a defined risk management process and understanding that educating and training people is every bit as important as the technology deployed. Incident rates and qualitative measures (such as the belief that the systems work well) support that conclusion. And with new technologies, including facial recognition and artificial intelligence just beginning to emerge, the trend points to a growing effectiveness in the future.

ACKNOWLEDGMENTS

Scott Briscoe, *content development director* at ASIS International, is the primary researcher and author of this report. He would like to acknowledge the following people who made incredible contributions to the research and analysis:

Stephen W. Di Rito
Vice President, Chief Security Officer
HealthPartners

Maria Dominguez
Senior Vice President, Business Support
Bank of America

Ross Johnson, CPP
President
Bridgehead Security Consulting

Parnell Lea
Director, Security & Life Safety
Brookfield Properties

Don McInnes, PSP
Physical Security & Fire Alarms Specialist
Instructor and Consultant

Sara Mosqueda
Associate Editor, Security Management
ASIS International

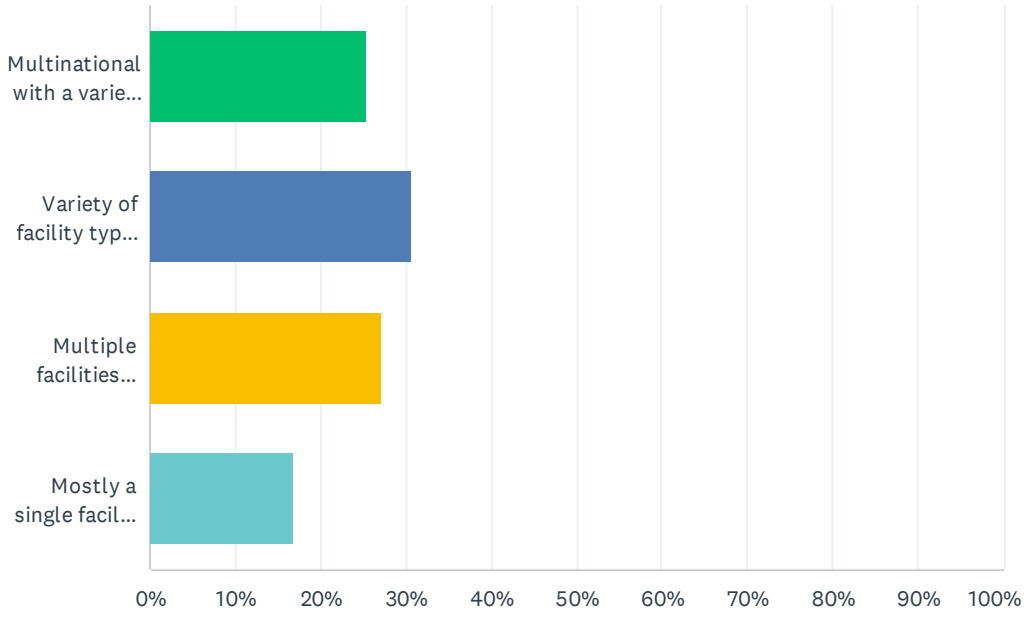
Jody Shaffer
Vice President, Marketing
FacilityOS Facility & Visitor Management

ADDENDUM: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q1 Which of the following best describes the scope of your security responsibilities?

Answered: 1,008 Skipped: 14



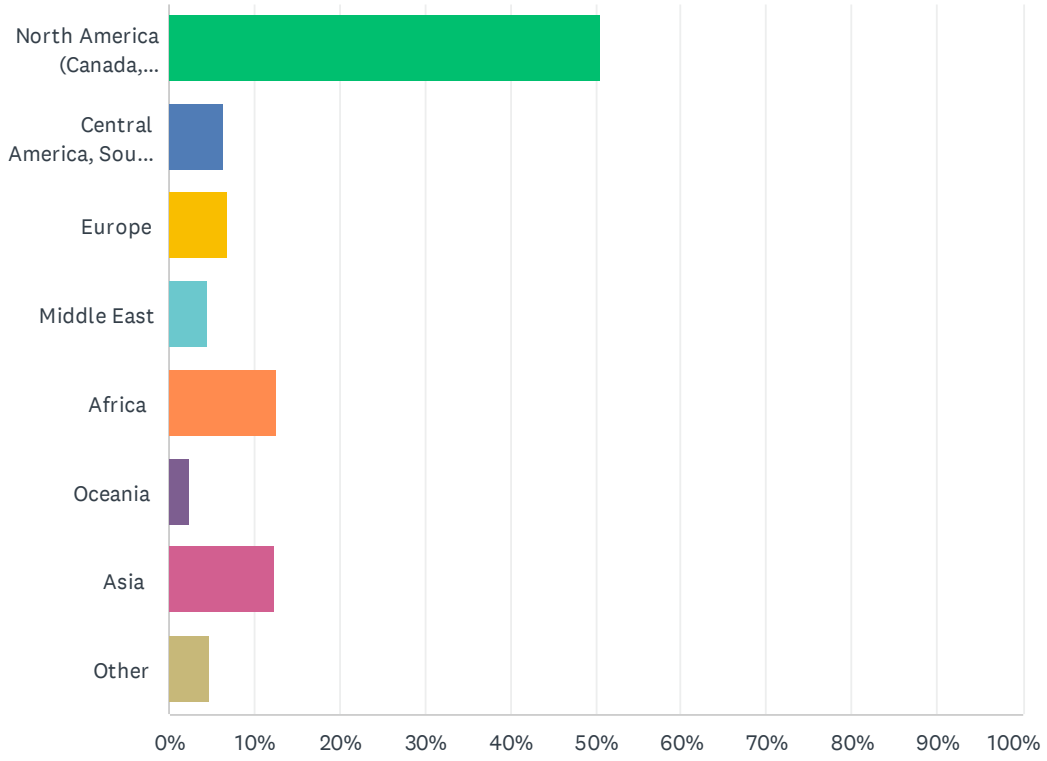
ANSWER CHOICES	RESPONSES	
Multinational with a variety of facility types in multiple countries	25.30%	255
Variety of facility types in multiple regions or locations primarily within a single country	30.75%	310
Multiple facilities primarily in a single region	27.08%	273
Mostly a single facility or single campus with a few facilities	16.87%	170
TOTAL		1,008

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q2 Where is your primary scope of security responsibility? (If 90% or more of your security scope falls within one of the regions below, please choose that region. If not, please choose “other.”)

Answered: 1,017 Skipped: 5



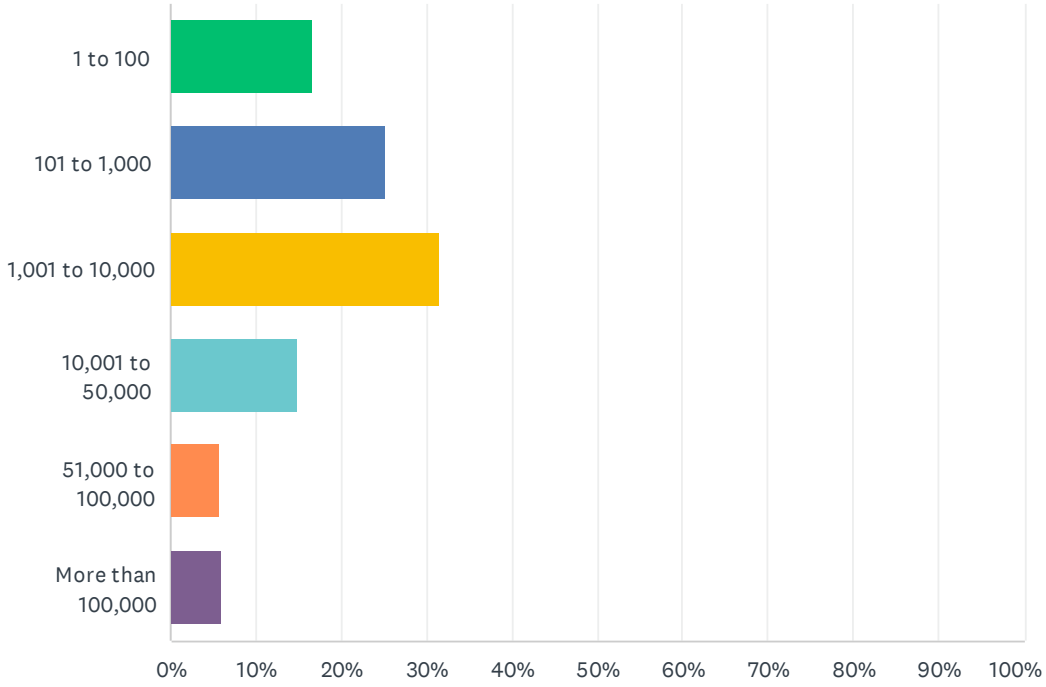
ANSWER CHOICES	RESPONSES	
North America (Canada, Mexico, United States)	50.54%	514
Central America, South America, and Caribbean	6.29%	64
Europe	6.88%	70
Middle East	4.52%	46
Africa	12.59%	128
Oceania	2.26%	23
Asia	12.29%	125
Other	4.62%	47
TOTAL		1,017

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q3 How many employees work at your organization?

Answered: 1,014 Skipped: 8



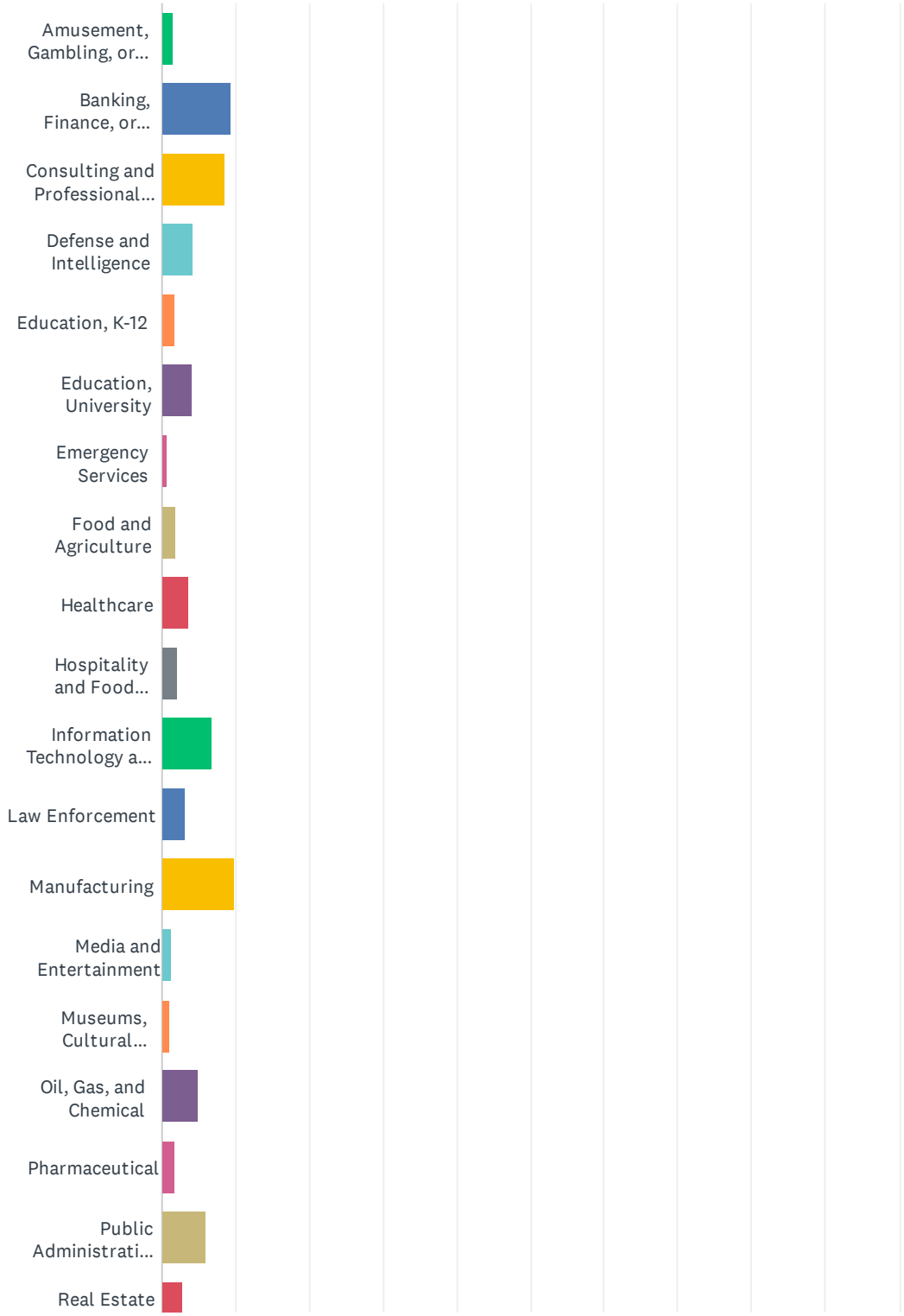
ANSWER CHOICES	RESPONSES	
1 to 100	16.57%	168
101 to 1,000	25.15%	255
1,001 to 10,000	31.56%	320
10,001 to 50,000	14.99%	152
51,000 to 100,000	5.82%	59
More than 100,000	5.92%	60
TOTAL		1,014

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

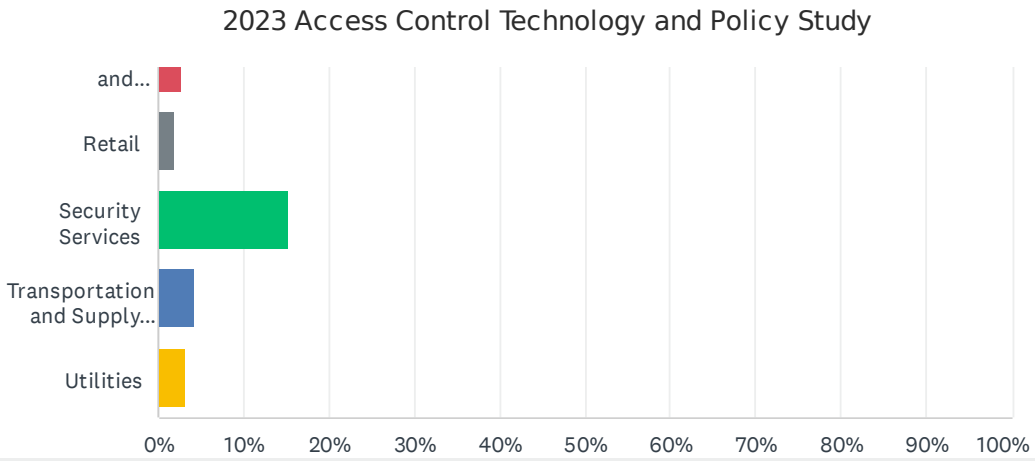
2023 Access Control Technology and Policy Study

Q4 Which of the following best describes your industry?

Answered: 1,017 Skipped: 5



ADDENDUM I: FULL SUMMARY SURVEY RESULTS



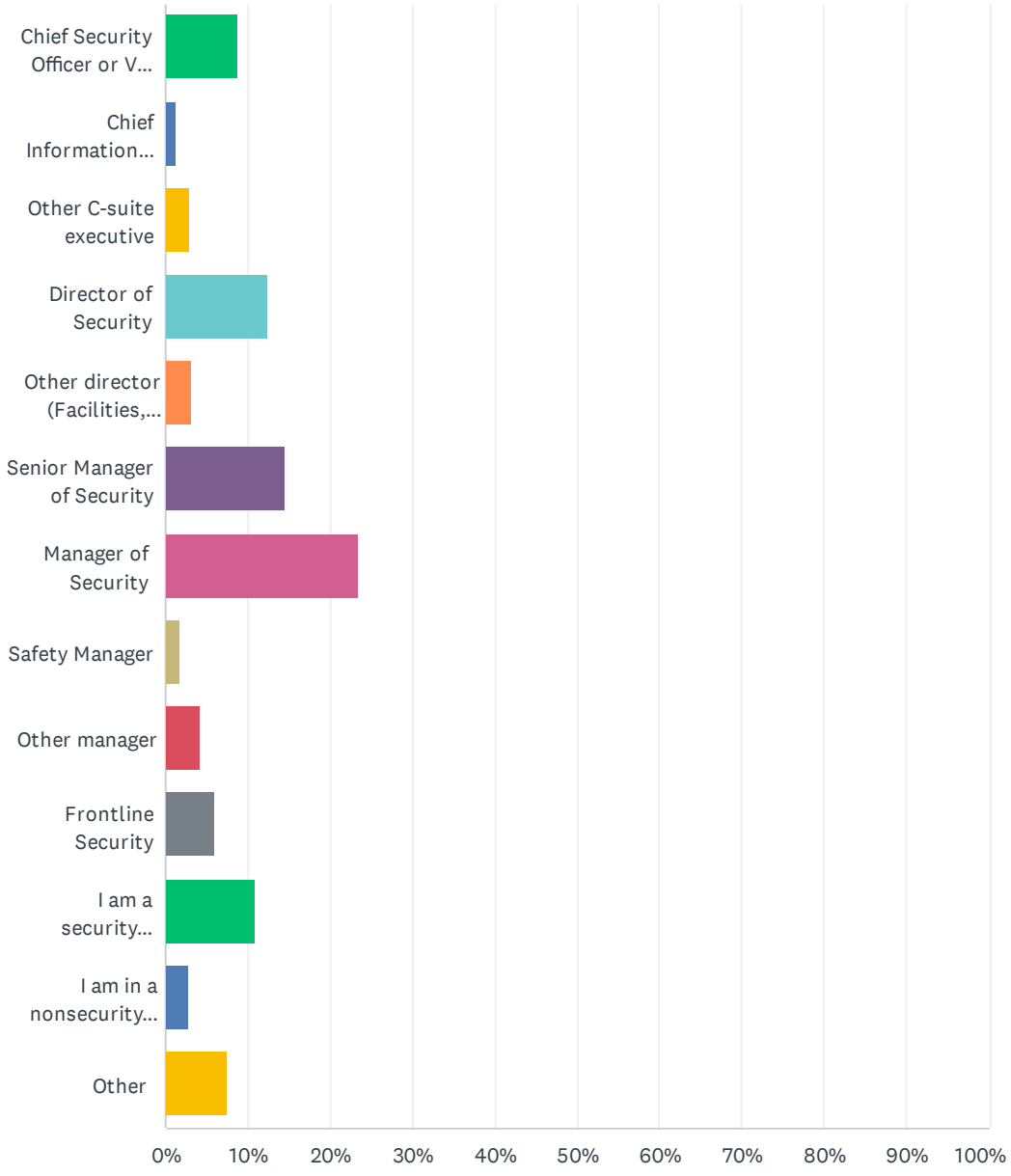
ANSWER CHOICES	RESPONSES	
Amusement, Gambling, or Recreation	1.57%	16
Banking, Finance, or Insurance	9.34%	95
Consulting and Professional Services	8.46%	86
Defense and Intelligence	4.33%	44
Education, K-12	1.67%	17
Education, University	4.13%	42
Emergency Services	0.59%	6
Food and Agriculture	1.87%	19
Healthcare	3.54%	36
Hospitality and Food Services	2.16%	22
Information Technology and Telecommunications	6.88%	70
Law Enforcement	3.24%	33
Manufacturing	9.73%	99
Media and Entertainment	1.18%	12
Museums, Cultural Properties	1.08%	11
Oil, Gas, and Chemical	4.92%	50
Pharmaceutical	1.77%	18
Public Administration/Government (Not defense, law enforcement, or education)	5.90%	60
Real Estate and Construction	2.85%	29
Retail	1.97%	20
Security Services	15.44%	157
Transportation and Supply Chain	4.23%	43
Utilities	3.15%	32
TOTAL		1,017

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q5 Please select the title that best describes your role:

Answered: 1,022 Skipped: 0



ADDENDUM I: FULL SUMMARY SURVEY RESULTS

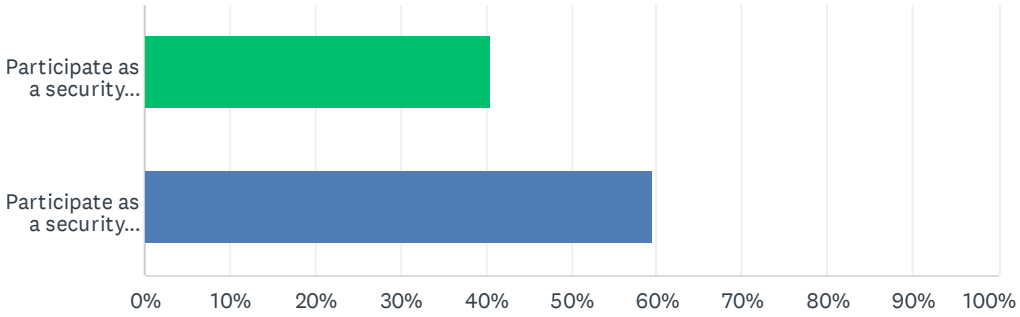
2023 Access Control Technology and Policy Study

ANSWER CHOICES	RESPONSES	
Chief Security Officer or VP of Security	8.81%	90
Chief Information Security Officer	1.27%	13
Other C-suite executive	2.94%	30
Director of Security	12.43%	127
Other director (Facilities, Risk, Compliance, etc.)	3.23%	33
Senior Manager of Security	14.58%	149
Manager of Security	23.48%	240
Safety Manager	1.76%	18
Other manager	4.31%	44
Frontline Security	5.97%	61
I am a security consultant.	10.86%	111
I am in a nonsecurity role at a company with products and services that aid a company's security	2.84%	29
Other	7.53%	77
TOTAL		1,022

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

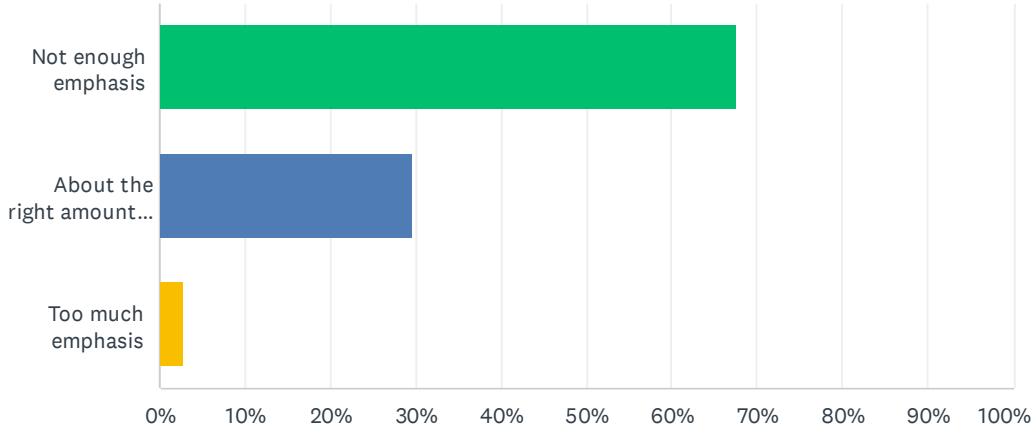
2023 Access Control Technology and Policy Study

Q6 Would you prefer to answer this survey as a security professional using your previous experience as a security professional as your guide, or, alternatively, would you prefer to answer a set of questions geared toward capturing the unique perspective of consultants and business partners serving the security profession?



ANSWER CHOICES	RESPONSES	
Participate as a security professional	40.44%	55
Participate as a security consultant or business partner	59.56%	81
TOTAL		136

Q7 In your experience, do companies tend to place too much or not enough emphasis on access control solutions?



ANSWER CHOICES	RESPONSES	
Not enough emphasis	67.61%	48
About the right amount of emphasis	29.58%	21
Too much emphasis	2.82%	2
TOTAL		71

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q8 Rank each of the following access control technical innovations on how important it is to effective access control.

Answered: 71 Skipped: 951

	1 - NOT AT ALL IMPORTANT	2	3	4	5 - MEDIUM LEVEL OF IMPORTANCE	6	7	8	9	10 - CRITICALL IMPORTAN
Mobile device credentials	4.23% 3	4.23% 3	7.04% 5	7.04% 5	14.08% 10	5.63% 4	16.90% 12	15.49% 11	8.45% 6	16.90% 1
Incorporating a Personal Identification and Access Management (PIAM) system	1.41% 1	0.00% 0	1.41% 1	2.82% 2	11.27% 8	7.04% 5	22.54% 16	12.68% 9	15.49% 11	25.35% 1
Linking access controls to critical systems such as IT access	0.00% 0	1.41% 1	1.41% 1	0.00% 0	9.86% 7	8.45% 6	11.27% 8	21.13% 15	21.13% 15	25.35% 1
Biometric access control	1.41% 1	2.82% 2	8.45% 6	9.86% 7	9.86% 7	5.63% 4	12.68% 9	12.68% 9	16.90% 12	19.72% 1
Using multifactor authentication for access control	1.41% 1	0.00% 0	2.82% 2	1.41% 1	9.86% 7	5.63% 4	14.08% 10	21.13% 15	18.31% 13	25.35% 1
Artificial intelligence or machine learning analysis of access control data	2.82% 2	7.04% 5	5.63% 4	1.41% 1	16.90% 12	11.27% 8	15.49% 11	16.90% 12	12.68% 9	9.86%
Access control system integration with surveillance system	0.00% 0	0.00% 0	1.41% 1	1.41% 1	1.41% 1	5.63% 4	7.04% 5	26.76% 19	14.08% 10	42.25% 3

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q9 Rank each of the following access control policies or procedures on how important it is to effective access control.

Answered: 71 Skipped: 951

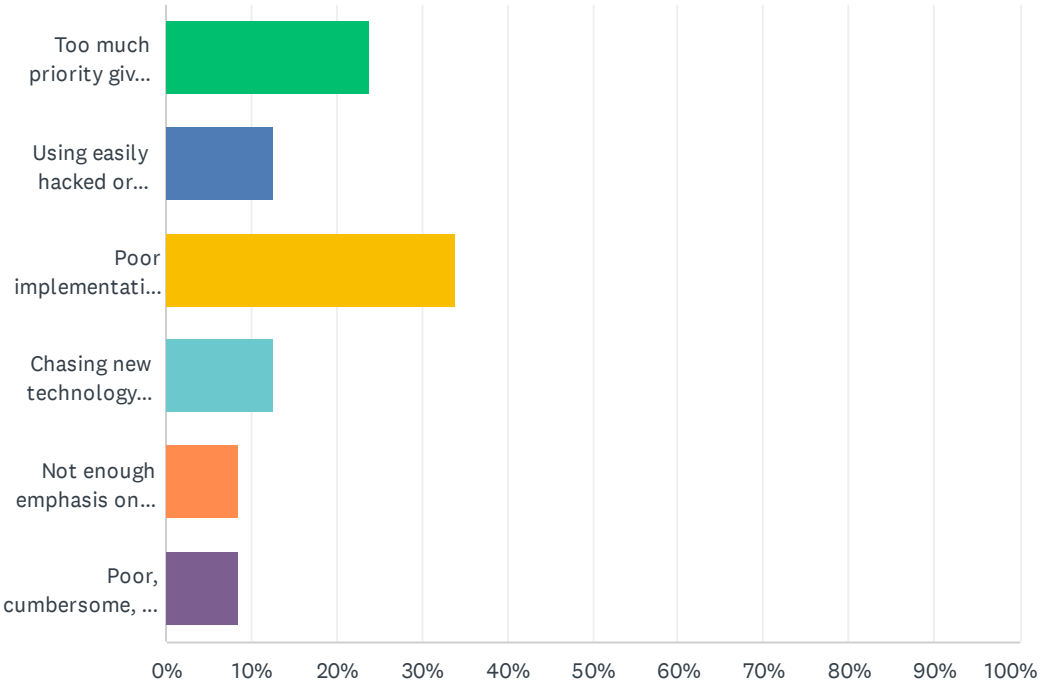
	1 - NOT AT ALL IMPORTANT	2	3	4	5 - MEDIUM LEVEL OF IMPORTANCE	6	7	8	9	10 - CRITICALLY IMPORTANT
Employing crime prevention through environmental design (CPTED)	1.41% 1	0.00% 0	1.41% 1	2.82% 2	12.68% 9	5.63% 4	14.08% 10	16.90% 12	16.90% 12	28.17% 20
Incorporating access control into the overall security risk management plan	0.00% 0	1.41% 1	0.00% 0	0.00% 0	4.23% 3	2.82% 2	2.82% 2	12.68% 9	21.13% 15	54.93% 39
Security Awareness training	0.00% 0	0.00% 0	1.41% 1	2.82% 2	2.82% 2	2.82% 2	9.86% 7	8.45% 6	22.54% 16	49.30% 35

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q10 In your experience, which of the following access control concerns or failures do you see the most? Choose only one

Answered: 71 Skipped: 951



ANSWER CHOICES	RESPONSES	
Too much priority given to employee convenience	23.94%	17
Using easily hacked or insecure technology	12.68%	9
Poor implementation of technology/choosing technology that is not correct for the situation	33.80%	24
Chasing new technology without a well thought out strategy	12.68%	9
Not enough emphasis on security awareness training	8.45%	6
Poor, cumbersome, or nonexistent visitor management system	8.45%	6
TOTAL		71

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q11 In your experience, do most security professionals do a good job using access control data?

Answered: 71 Skipped: 951

2.9★

average rating

	DO A VERY POOR JOB	DO THE BARE MINIMUM	DO AN ADEQUATE JOB	DO A GOOD JOB	DO AN EXCELLENT JOB	TOTAL	WEIGHTED AVERAGE
☆	4.23% 3	26.76% 19	40.85% 29	26.76% 19	1.41% 1	71	2.94

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q12 What is the most exciting or impactful recent access control development?

Answered: 65 Skipped: 957

Various Open-ended Answsers

2023 Access Control Technology and Policy Study

Q13 What is the one piece of advice you would give to security professionals about access control?

Answered: 62 Skipped: 960

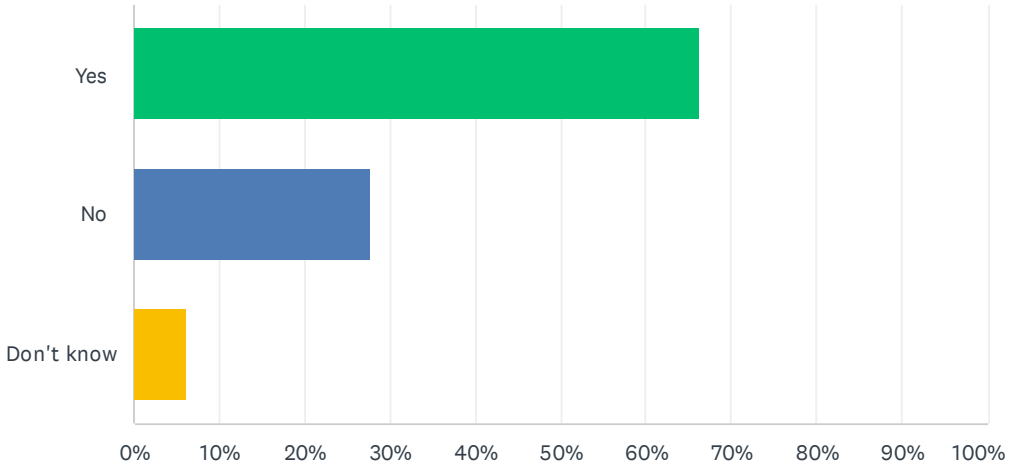
Various Open-ended Answsers

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q14 Is your organization required by statute or other regulatory compliance measures to meet certain access control standards?

Answered: 937 Skipped: 85



ANSWER CHOICES	RESPONSES	
Yes	66.28%	621
No	27.64%	259
Don't know	6.08%	57
TOTAL		937

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q15 Which standards apply to your access control solution? Choose all that apply

Answered: 590 Skipped: 432

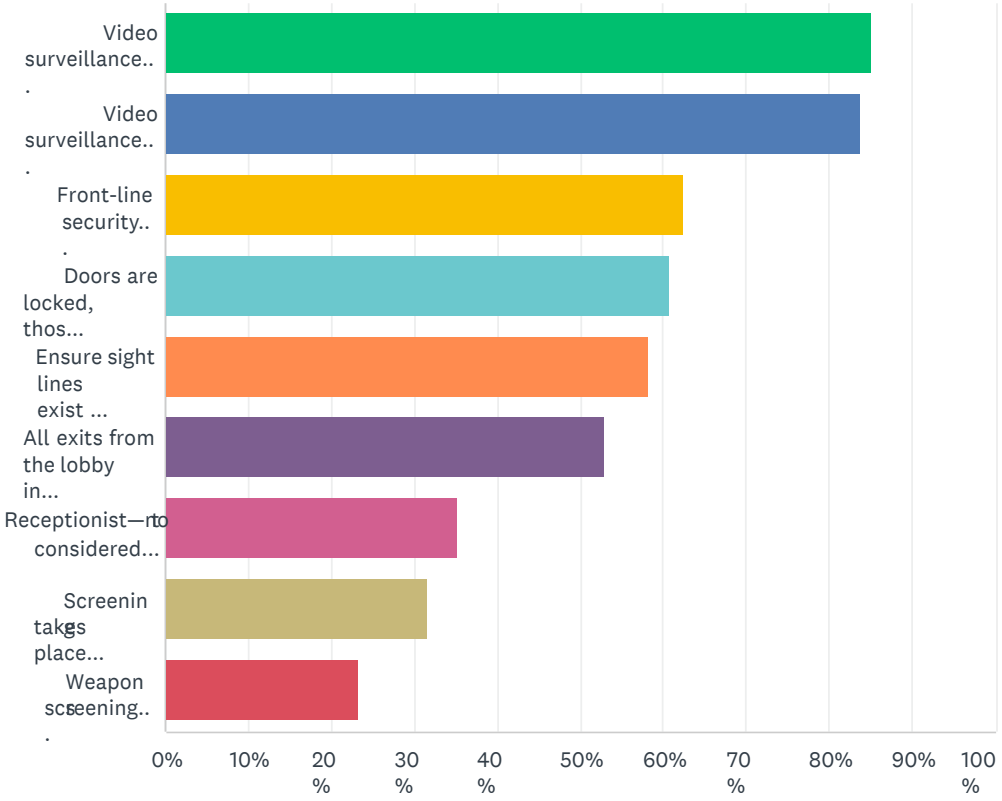
ANSWER CHOICES	RESPONSES	
Other government agency regulations	42.03%	248
ISO-9001	29.15%	172
OSHA regulations	27.46%	162
Other (please specify)	18.98%	112
GDPR	17.80%	105
Federal standards—FIPS201/HSPD12	16.95%	100
Department of Defense/Military regulations	16.27%	96
Classified Space	13.22%	78
CT-PAT	9.83%	58
PCI-DSS	8.47%	50
SOC2-Type 2	7.63%	45
Department of Energy regulations	5.42%	32
Food Safety Modernization Act	5.08%	30
NERC CIP Standards	4.75%	28
GMP Standards	4.41%	26
California Consumer Privacy Act	4.24%	25
Gramm-Leach-Bliley Act	3.05%	18
FISMA	2.71%	16
Total Respondents: 590		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q16 Which of the following security measures are at your primary entrances? Choose all that apply (If you have multiple facilities, please answer for your primary or headquarters facility.)

Answered: 856 Skipped: 166



ANSWER CHOICES	RESPONSES	
Video surveillance inside	85.16%	729
Video surveillance outside	83.76%	717
Front-line security officer(s) (either serving as receptionist or stationed at entrance)	62.50%	535
Doors are locked, those without credentials must be allowed in manually	60.86%	521
Ensure sight lines exist so people approaching facility are visible	58.18%	498
All exits from the lobby into the facility, including stairwells and elevators, are only accessible with credentials	52.92%	453
Receptionist—not considered front-line security officer	35.16%	301
Screening takes place outside the facility, only those with permission are allowed to approach the facility	31.66%	271
Weapons screening technology	23.25%	199

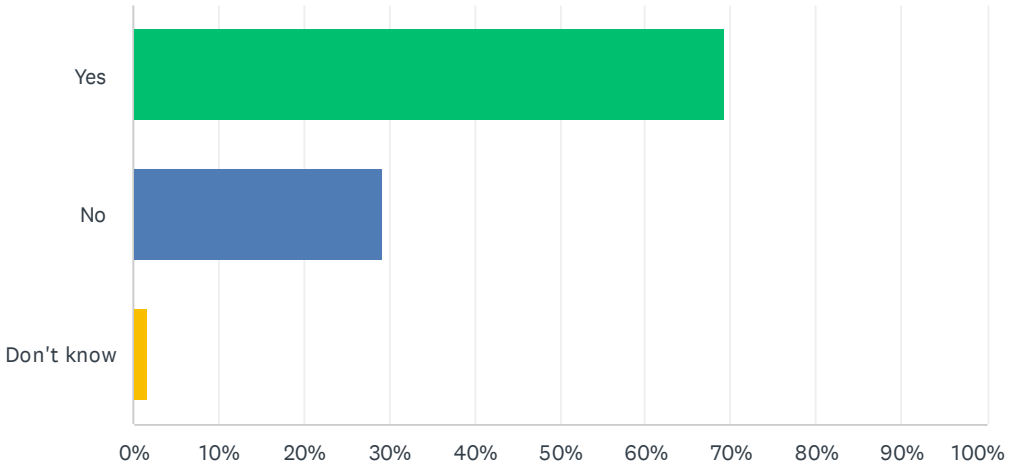
Total Respondents: 856

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q17 Do you have secondary entrances/exits that are regularly used (e.g. they are not for emergencies only)?

Answered: 857 Skipped: 165



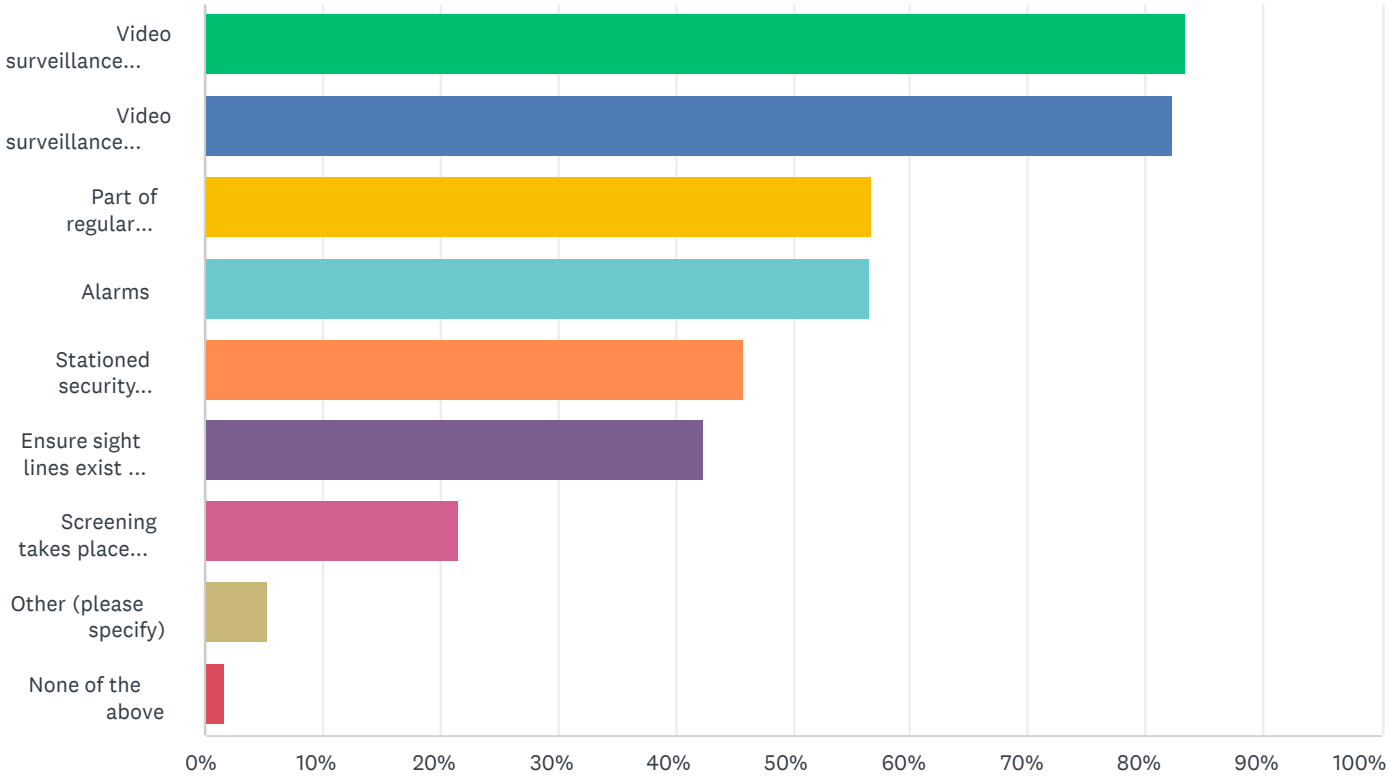
ANSWER CHOICES	RESPONSES	
Yes	69.19%	593
No	29.17%	250
Don't know	1.63%	14
TOTAL		857

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q18 Other than the use of card/biometric/mobile credentials, what security measures are in place at these secondary entrances/exits? Choose all that apply

Answered: 578 Skipped: 444



ANSWER CHOICES	RESPONSES	
Video surveillance outside	83.39%	482
Video surveillance inside	82.35%	476
Part of regular security patrols	56.75%	328
Alarms	56.40%	326
Stationed security personnel	45.85%	265
Ensure sight lines exist so people approaching facility are visible	42.39%	245
Screening takes place outside the facility, only those with permission are allowed to approach the facility	21.45%	124
Other (please specify)	5.36%	31
None of the above	1.73%	10

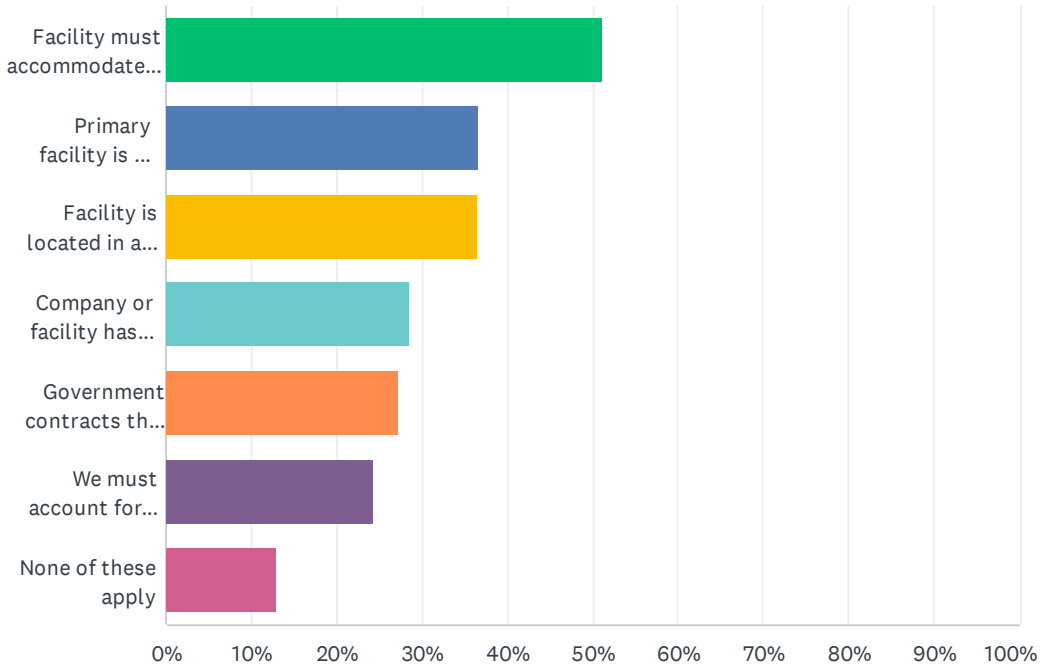
Total Respondents: 578

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q19 Do you face any of these special security scenarios? Choose all that apply

Answered: 816 Skipped: 206



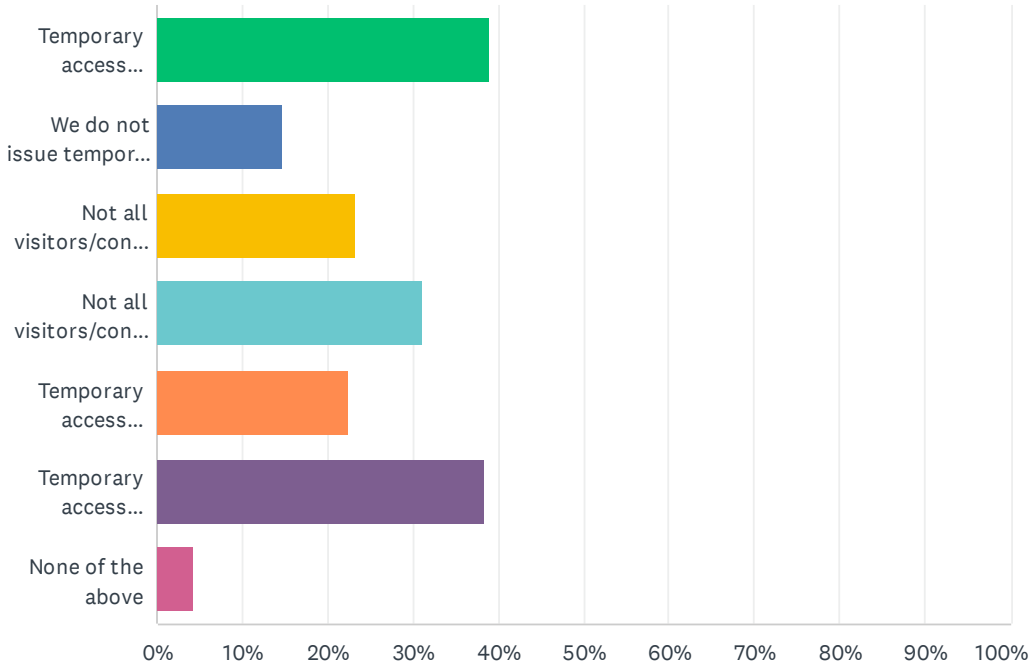
ANSWER CHOICES	RESPONSES	
Facility must accommodate public access	51.23%	418
Primary facility is a shared facility with one or more other companies	36.76%	300
Facility is located in an area prone to high-crime activity, violence, or civil unrest	36.40%	297
Company or facility has been the target of protests or violence	28.68%	234
Government contracts that require special access control or security features	27.33%	223
We must account for hazardous or federally controlled substances	24.26%	198
None of these apply	12.99%	106
Total Respondents: 816		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q20 Which of the following are characteristics of the temporary access credentials you issue to visitors? Choose all that apply

Answered: 821 Skipped: 201



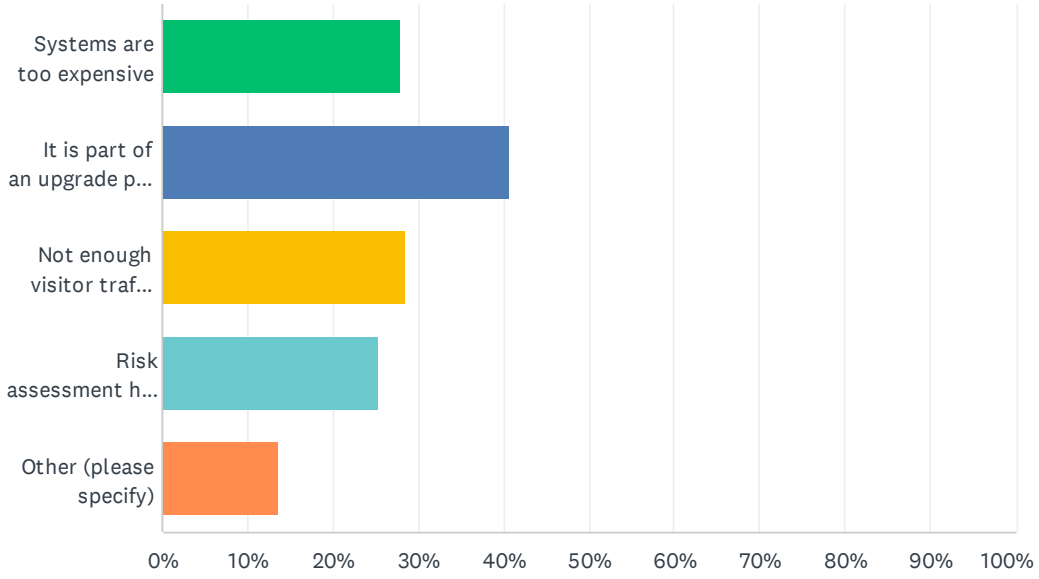
ANSWER CHOICES	RESPONSES	
Temporary access credentials are tracked using a manual system (pen-and-paper or spreadsheet)	38.98%	320
We do not issue temporary access credentials	14.74%	121
Not all visitors/contractors/temps receive access credentials, mostly dependent on length of visit	23.14%	190
Not all visitors/contractors/temps receive access credentials, mostly dependent on access needs	31.06%	255
Temporary access credentials are tied to a visitor's personal identity via PIAM system.	22.29%	183
Temporary access credentials are tracked using our access control system (a system more limited than PIAM)	38.37%	315
None of the above	4.26%	35
Total Respondents: 821		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q21 Why don't you use a dedicated digital system to track temporary access credentials? Choose all that apply

Answered: 409 Skipped: 613



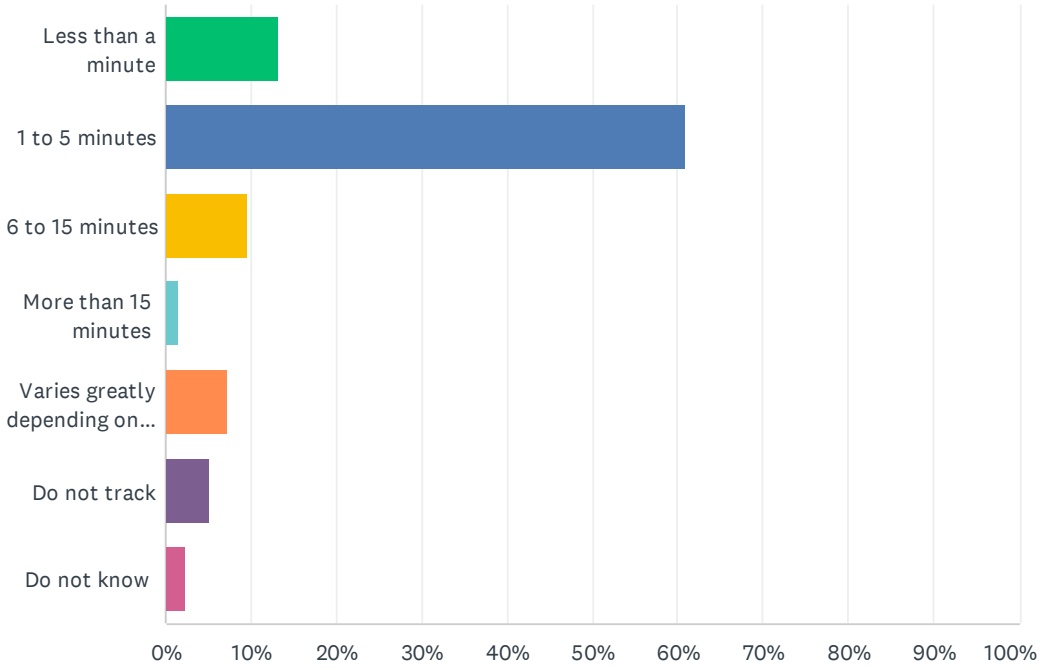
ANSWER CHOICES	RESPONSES	
Systems are too expensive	27.87%	114
It is part of an upgrade plan that has not been installed yet	40.83%	167
Not enough visitor traffic to warrant a dedicated system	28.61%	117
Risk assessment has not identified this as a priority	25.43%	104
Other (please specify)	13.69%	56
Total Respondents: 409		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q22 On average, how long does it take you to process a temporary or short-term visitor? Choose one

Answered: 783 Skipped: 239



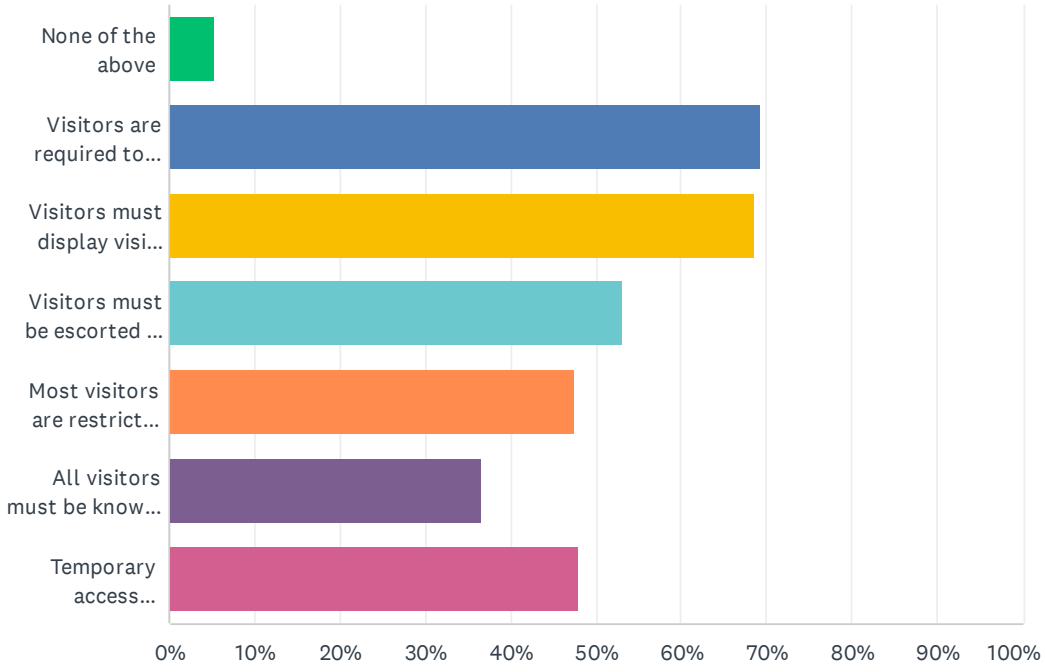
ANSWER CHOICES	RESPONSES	
Less than a minute	13.28%	104
1 to 5 minutes	60.92%	477
6 to 15 minutes	9.58%	75
More than 15 minutes	1.53%	12
Varies greatly depending on circumstances	7.15%	56
Do not track	5.11%	40
Do not know	2.43%	19
TOTAL		783

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q23 Which of the following visitor management policies or practices do you employ? Choose all that apply

Answered: 781 Skipped: 241



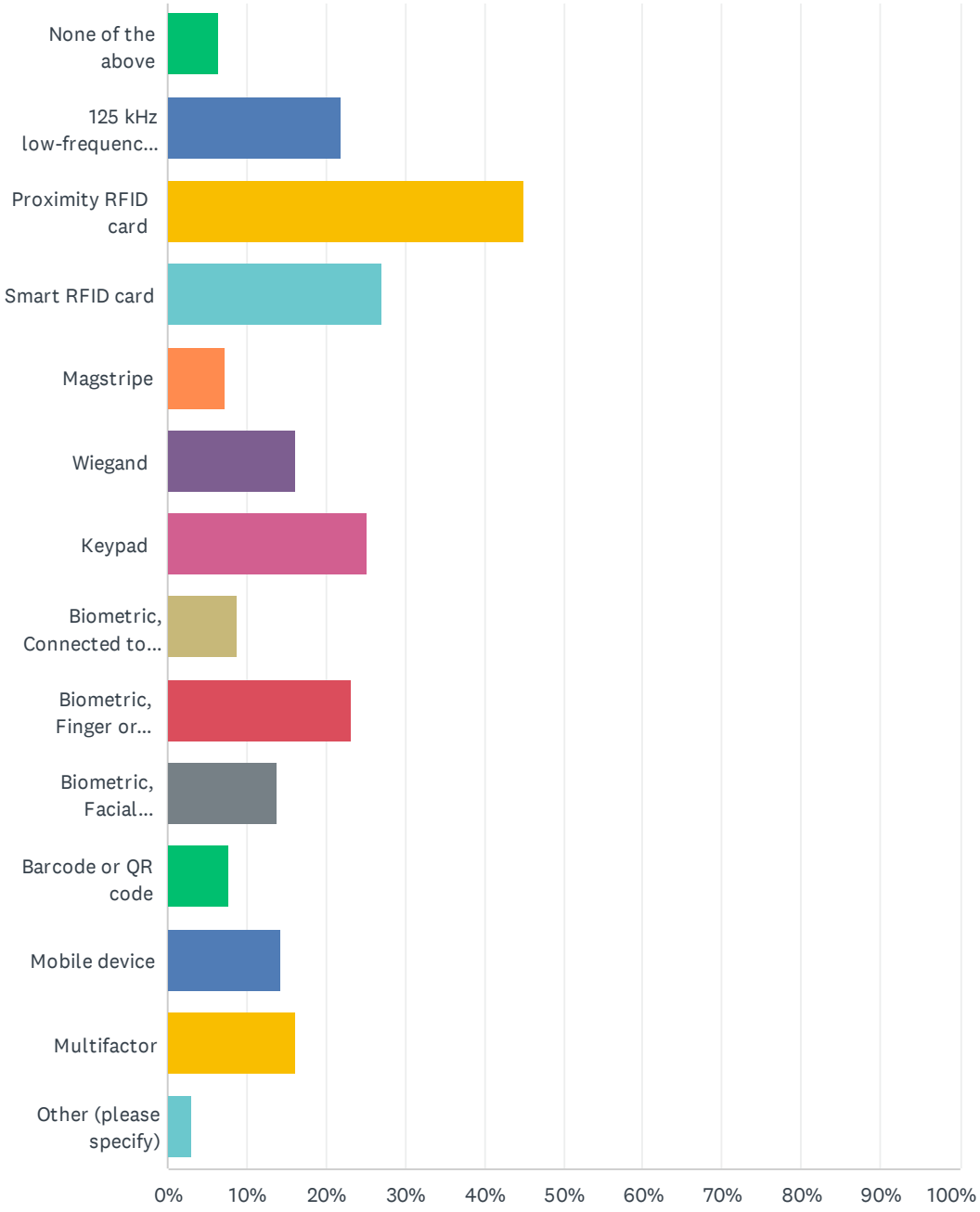
ANSWER CHOICES	RESPONSES	
None of the above	5.25%	41
Visitors are required to show valid, government-issued identification	69.27%	541
Visitors must display visitor badge, sticker, or pin	68.63%	536
Visitors must be escorted at all times	53.14%	415
Most visitors are restricted to offices or conference rooms near the main entrance unless there is an express need to access other parts of the facility	47.50%	371
All visitors must be known in advance and be prescreened by security	36.62%	286
Temporary access credentials must be approved by security or centralized authority	47.89%	374
Total Respondents: 781		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q24 What kind of access control credentialing technology do you employ? Choose all that apply

Answered: 782 Skipped: 240



ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

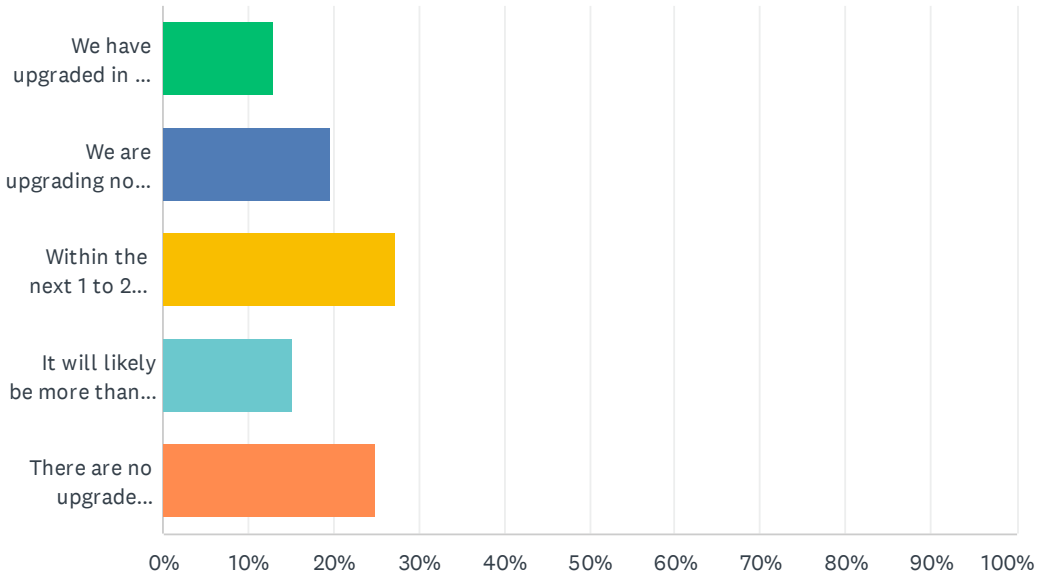
ANSWER CHOICES	RESPONSES	
None of the above	6.39%	50
125 kHz low-frequency proximity card	21.99%	172
Proximity RFID card	45.01%	352
Smart RFID card	27.11%	212
Magstripe	7.29%	57
Wiegand	16.24%	127
Keypad	25.19%	197
Biometric, Connected to mobile device	8.82%	69
Biometric, Finger or handprint	23.27%	182
Biometric, Facial recognition or iris scan	13.94%	109
Barcode or QR code	7.67%	60
Mobile device	14.19%	111
Multifactor	16.11%	126
Other (please specify)	2.94%	23
Total Respondents: 782		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q25 When do you think you will make your next major upgrade to your access control technology? Choose one

Answered: 778 Skipped: 244



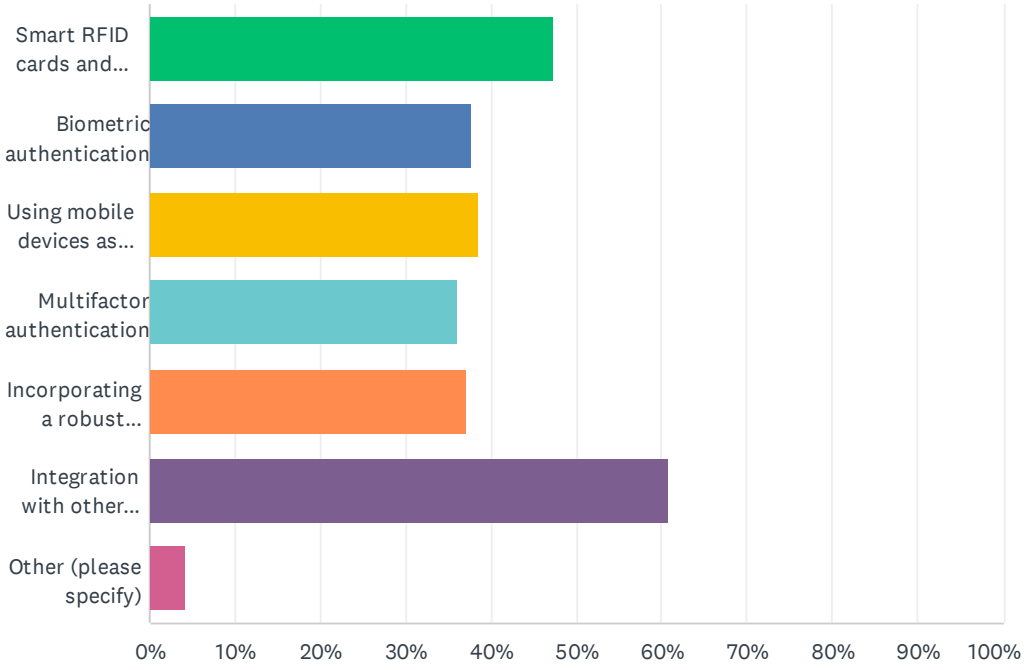
ANSWER CHOICES	RESPONSES	
We have upgraded in the past 12 months and do not need another upgrade yet	13.11%	102
We are upgrading now or will be in the next 6 months.	19.54%	152
Within the next 1 to 2 years	27.38%	213
It will likely be more than 2 years from now	15.04%	117
There are no upgrade plans/unsure	24.94%	194
TOTAL		778

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q26 Which features are most important for your next access control technology upgrade (for those who just upgraded, what features did you include in the upgrade)? Choose all that apply

Answered: 581 Skipped: 441



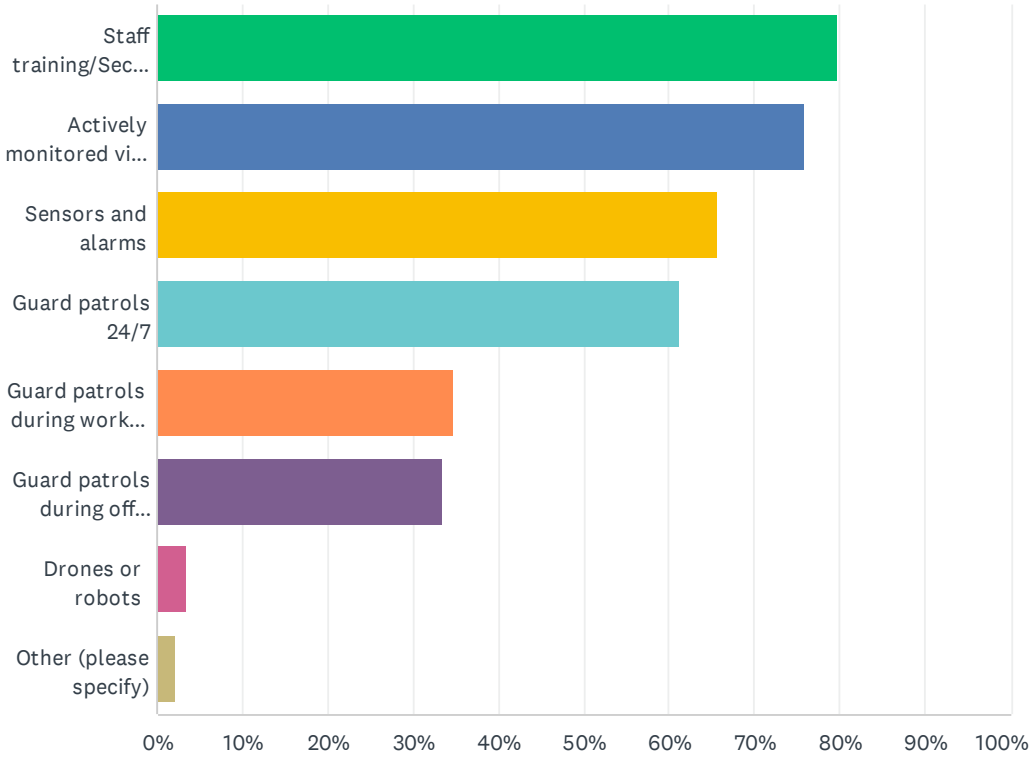
ANSWER CHOICES	RESPONSES	
Smart RFID cards and readers	47.33%	275
Biometric authentication	37.69%	219
Using mobile devices as credentials	38.55%	224
Multifactor authentication	35.97%	209
Incorporating a robust physical identity and access management (PIAM) solution	37.01%	215
Integration with other systems	60.76%	353
Other (please specify)	4.30%	25
Total Respondents: 581		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q27 What methods do you employ to ensure the access management system has not been breached? Choose all that apply

Answered: 733 Skipped: 289



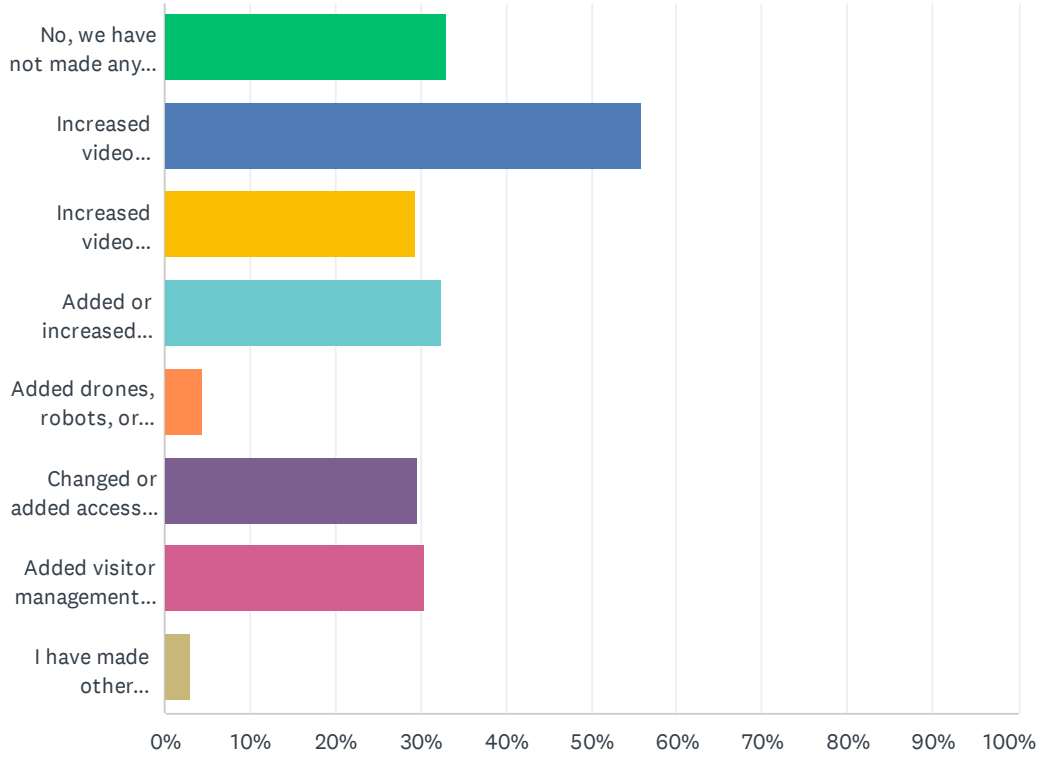
ANSWER CHOICES	RESPONSES	
Staff training/Security Awareness training	79.81%	585
Actively monitored video surveillance	75.85%	556
Sensors and alarms	65.62%	481
Guard patrols 24/7	61.12%	448
Guard patrols during work hours	34.79%	255
Guard patrols during off hours	33.56%	246
Drones or robots	3.41%	25
Other (please specify)	2.18%	16
Total Respondents: 733		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q28 Within the last 5 years have you employed technology solutions to reduce the security staff time needed to prevent or monitor unauthorized physical access? Choose all that apply

Answered: 726 Skipped: 296



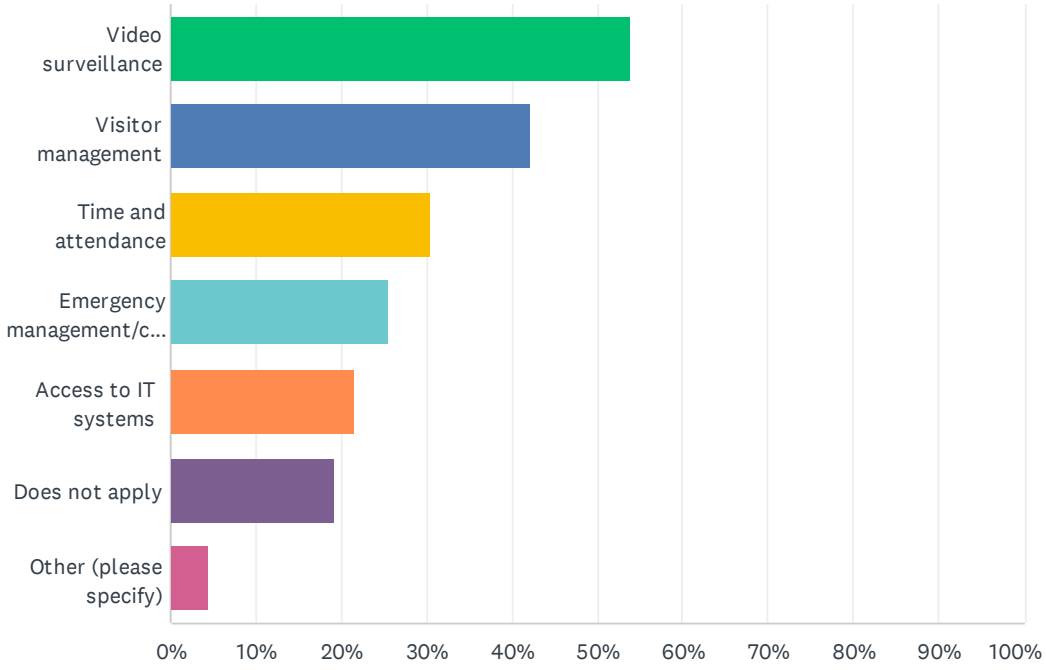
ANSWER CHOICES	RESPONSES	
No, we have not made any attempt to reduce the staff time needed to prevent or monitor unauthorized access.	33.06%	240
Increased video surveillance capacity: more cameras and/or more active video monitoring	55.79%	405
Increased video surveillance capability: use AI, improved cameras	29.48%	214
Added or increased sensors or alarms	32.37%	235
Added drones, robots, or related technology	4.41%	32
Changed or added access control technology to reduce staff needed at access points	29.61%	215
Added visitor management system to reduce staff time needed to process visitors	30.58%	222
I have made other modification to reduce the staff time needed. Please explain	2.89%	21
Total Respondents: 726		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q29 Is your access control technology integrated with any other technology systems? Choose all that apply

Answered: 724 Skipped: 298



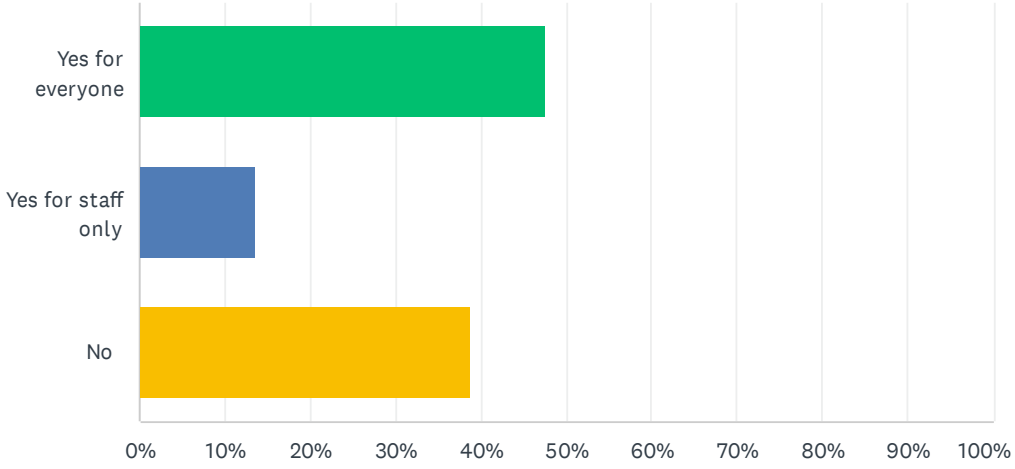
ANSWER CHOICES	RESPONSES	
Video surveillance	54.01%	391
Visitor management	42.13%	305
Time and attendance	30.52%	221
Emergency management/communication	25.69%	186
Access to IT systems	21.55%	156
Does not apply	19.20%	139
Other (please specify)	4.42%	32
Total Respondents: 724		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q30 Does your access control technology track both entry and exit so you know who is in the facility at any point in time?

Answered: 732 Skipped: 290



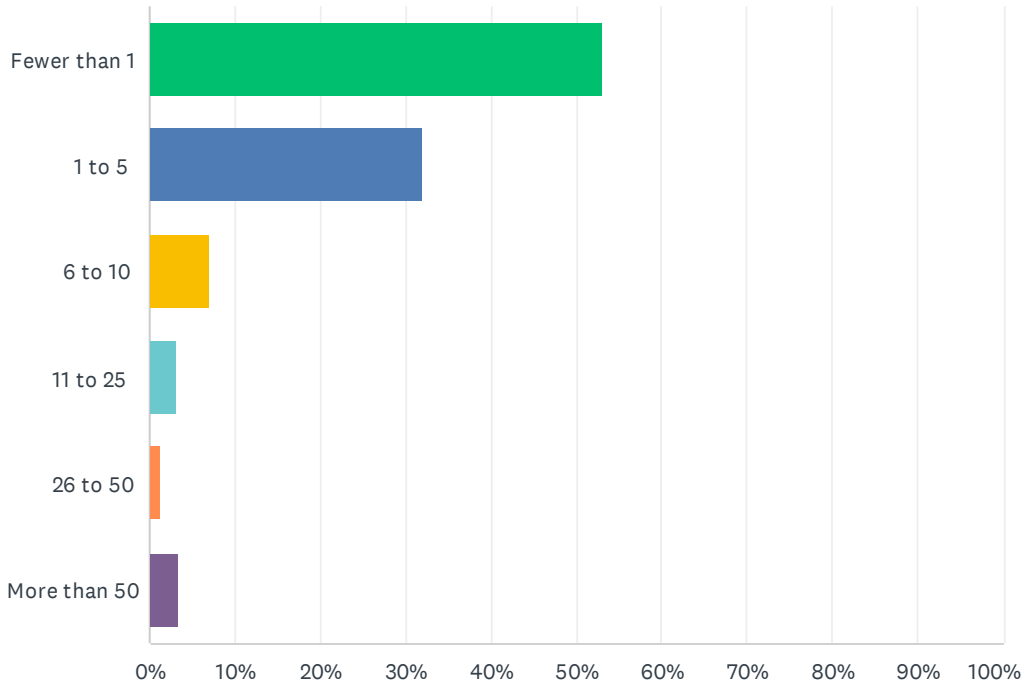
ANSWER CHOICES	RESPONSES	
Yes for everyone	47.63%	341
Yes for staff only	13.55%	97
No	38.83%	278
TOTAL		716

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q31 How many security incidents related to access control or unauthorized physical access do you face per week on average? Choose one (An “incident” is anything that requires security to take extra action to investigate or remediate.)

Answered: 732 Skipped: 290



ANSWER CHOICES	RESPONSES	
Fewer than 1	53.19%	350
1 to 5	31.91%	210
6 to 10	6.99%	46
11 to 25	3.19%	21
26 to 50	1.37%	9
More than 50	3.34%	22
TOTAL		658

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

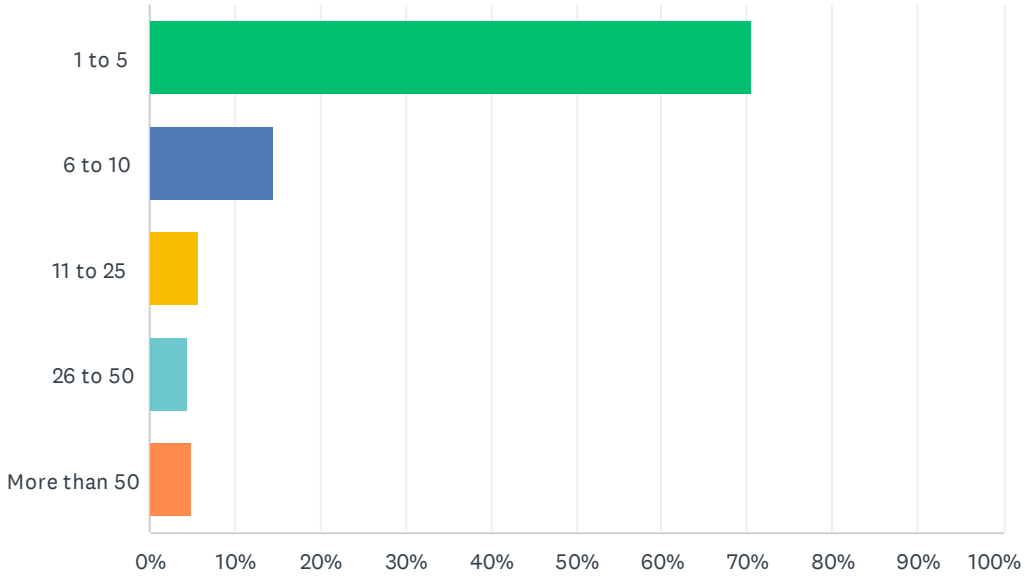
Q32 What percentage of those incidents are false alarms or very minor incidents? Choose a whole number between 0 and 100 (Leave blank if you do not know)

Answered: 421 Skipped: 601

Various Open-Ended Answers

Q33 On average, how many critical or serious access control or unauthorized physical access incidents do you face each year? Choose one

Answered: 709 Skipped: 313



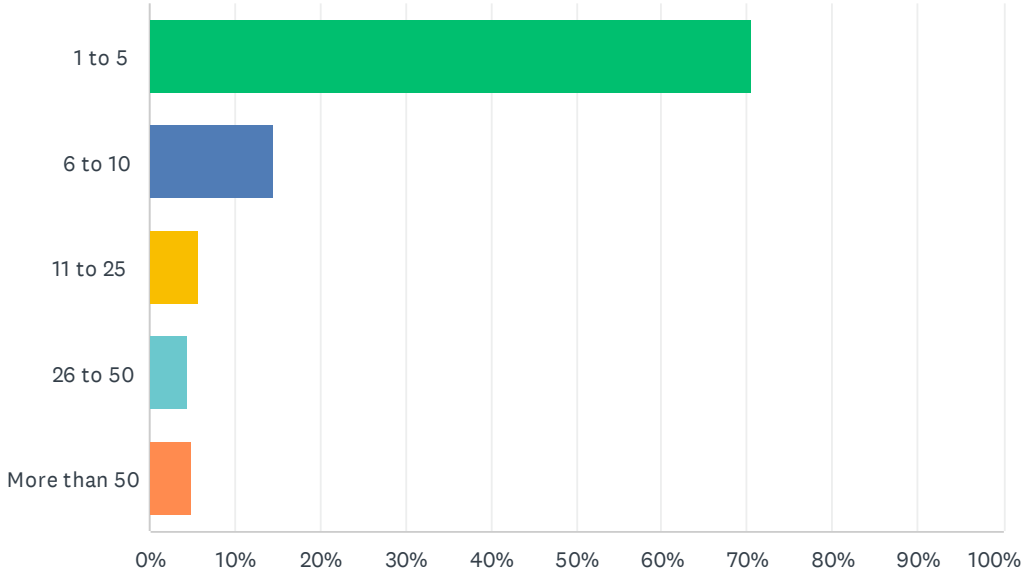
ANSWER CHOICES	RESPONSES	
1 to 5	70.50%	435
6 to 10	14.42%	89
11 to 25	5.83%	36
26 to 50	4.38%	27
More than 50	4.86%	30
TOTAL		617

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q33 On average, how many critical or serious access control or unauthorized physical access incidents do you face each year? Choose one

Answered: 709 Skipped: 313

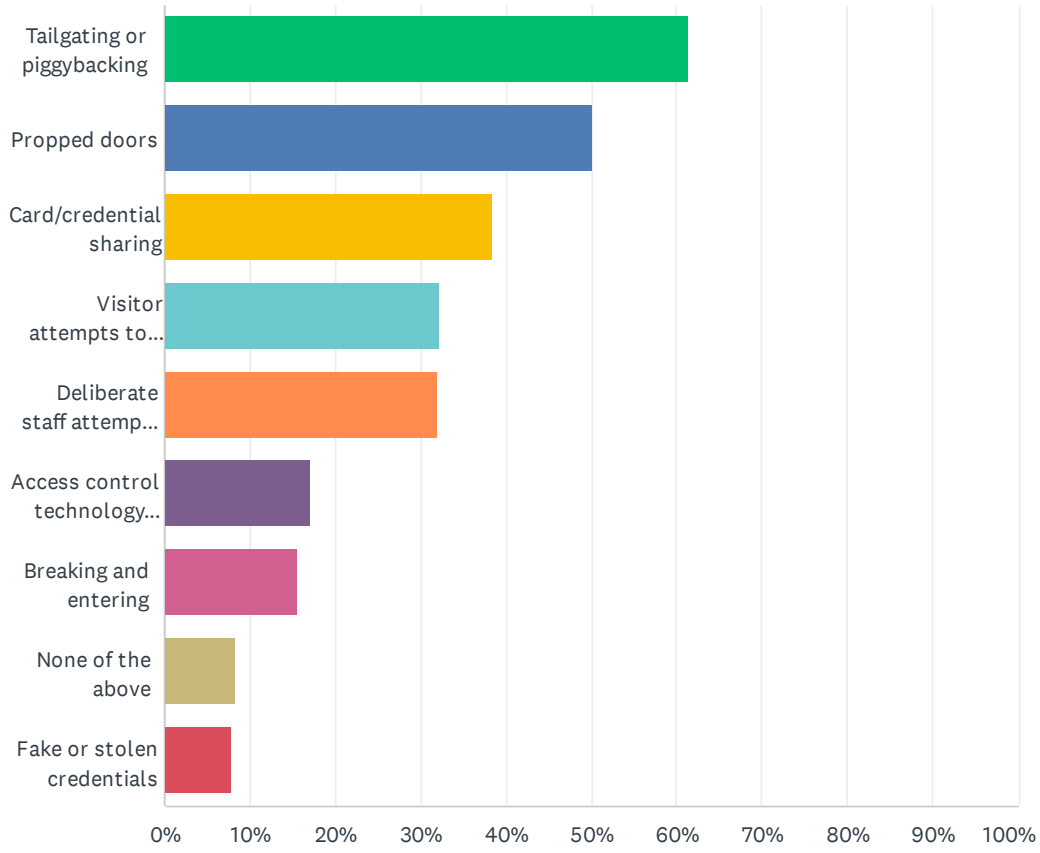


ANSWER CHOICES	RESPONSES	
1 to 5	70.50%	435
6 to 10	14.42%	89
11 to 25	5.83%	36
26 to 50	4.38%	27
More than 50	4.86%	30
TOTAL		617

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q34 Which of the following common access control incidents have occurred at your facility in the past 6 months? Choose all that apply



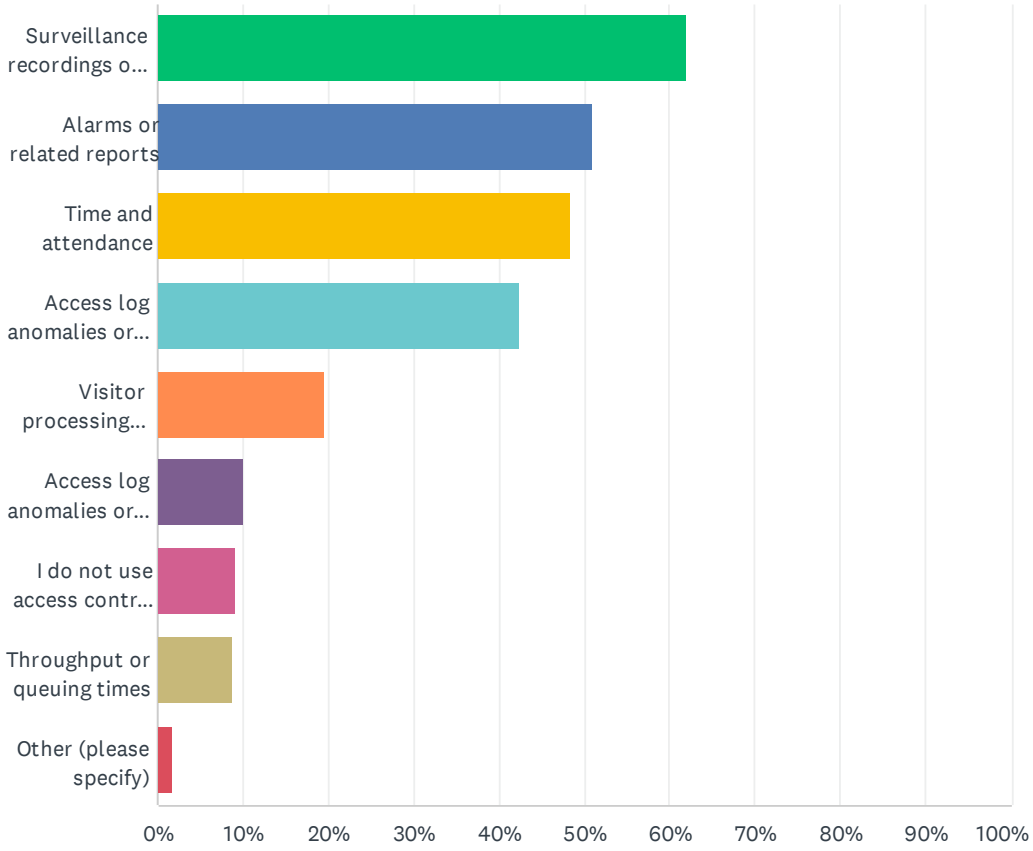
ANSWER CHOICES	RESPONSES	
Tailgating or piggybacking	61.42%	433
Propped doors	50.21%	354
Card/credential sharing	38.30%	270
Visitor attempts to circumvent procedures	32.20%	227
Deliberate staff attempts to circumvent procedures	31.91%	225
Access control technology failure resulting in unauthorized access	17.02%	120
Breaking and entering	15.46%	109
None of the above	8.23%	58
Fake or stolen credentials	7.80%	55
Total Respondents: 705		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q35 What access control-related data do you use?

Answered: 707 Skipped: 315



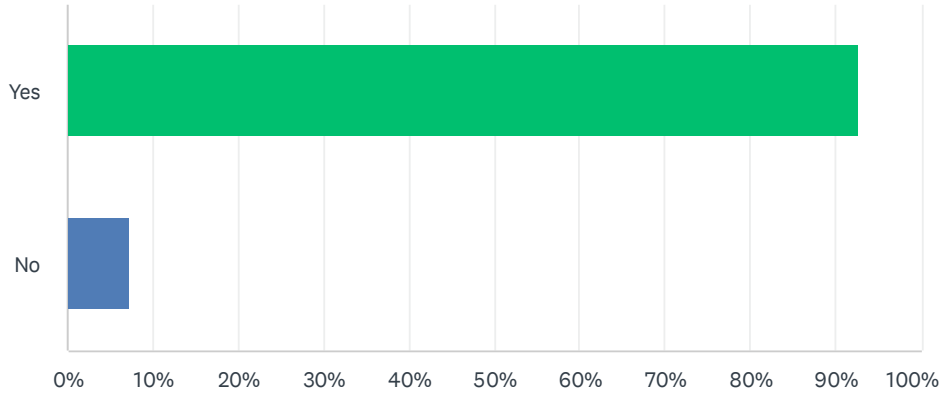
ANSWER CHOICES	RESPONSES	
Surveillance recordings of access points	61.95%	438
Alarms or related reports	51.06%	361
Time and attendance	48.37%	342
Access log anomalies or issues identified manually	42.43%	300
Visitor processing times	19.52%	138
Access log anomalies or issues identified by AI or machine learning	10.04%	71
I do not use access control data	9.19%	65
Throughput or queuing times	8.77%	62
Other (please specify)	1.70%	12
Total Respondents: 707		

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q36 Is access control an explicit part of a risk management or security plan at your organization?

Answered: 707 Skipped: 315



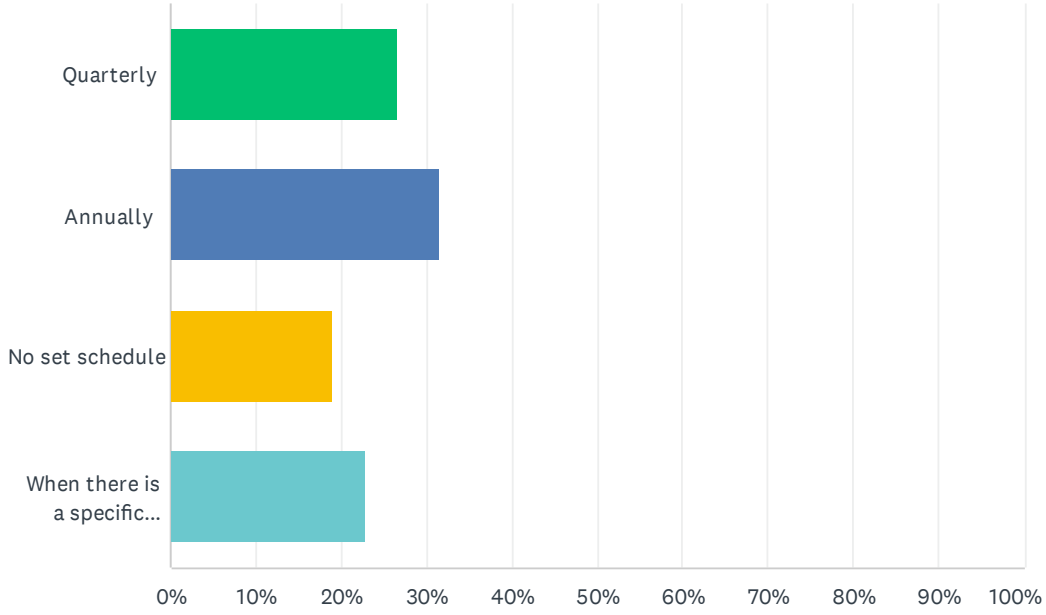
ANSWER CHOICES	RESPONSES	
Yes	92.80%	632
No	7.20%	49
TOTAL		681

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q37 How often is the access control part of the plan re-examined?

Answered: 629 Skipped: 393



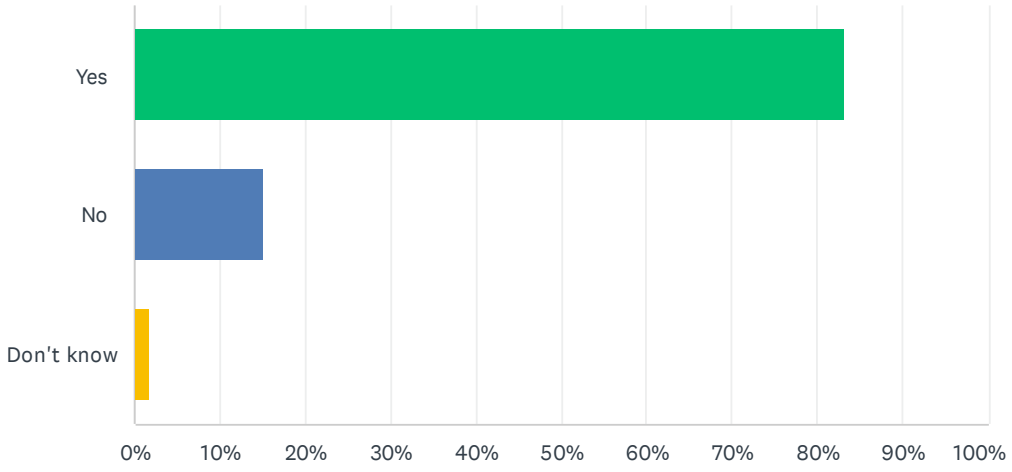
ANSWER CHOICES	RESPONSES	
Quarterly	26.55%	167
Annually	31.64%	199
No set schedule	19.08%	120
When there is a specific reason (such as after an incident or when the threat landscape has changed significantly)	22.73%	143
TOTAL		629

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q38 Does your facility have varying levels of access controls based on the risk profile of the asset being protected?

Answered: 667 Skipped: 355



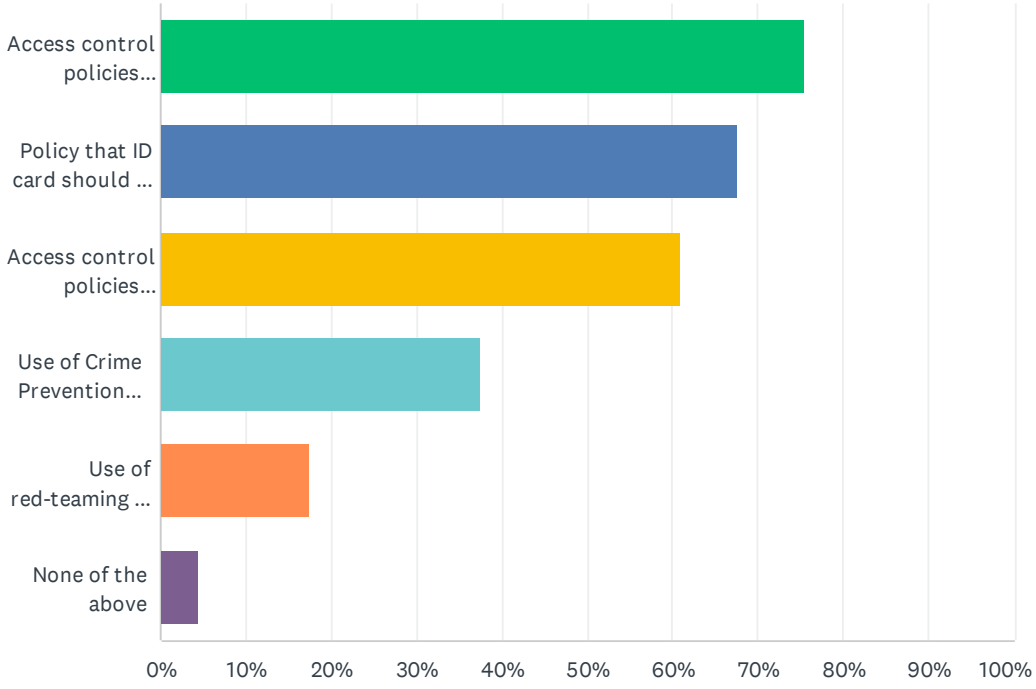
ANSWER CHOICES	RESPONSES	
Yes	83.06%	554
No	15.14%	101
Don't know	1.80%	12
TOTAL		667

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q39 Which of the following access controls policies or procedures does your organization employ? Choose all that apply

Answered: 667 Skipped: 355



ANSWER CHOICES	RESPONSES	
Access control policies emphasized as part of employee orientation	75.41%	503
Policy that ID card should be displayed at all times	67.62%	451
Access control policies emphasized regularly for all employees	61.02%	407
Use of Crime Prevention Through Environmental Design (CPTED) principles as a critical component to the overall access control design.	37.63%	251
Use of red-teaming to find access control technology or policy weaknesses	17.39%	116
None of the above	4.50%	30

Total Respondents: 667

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q40 Please indicate how strongly you agree with each of the following statements.

Answered: 664 Skipped: 358

	STRONGLY DISAGREE	DISAGREE	COULD GO EITHER WAY	AGREE	STRONGLY AGREE	TOTAL	WEIGHTED AVERAGE
I am confident our access control system meets all necessary requirements for employees	5.80% 38	11.15% 73	15.42% 101	42.29% 277	25.34% 166	655	3.70
I am confident our access control system meets all necessary requirements for visitor, contractor, and temporary staff management	7.66% 50	14.55% 95	16.85% 110	40.89% 267	20.06% 131	653	3.51
I am confident our access control system is highly effective at protecting the organization	6.30% 41	11.52% 75	20.89% 136	40.86% 266	20.43% 133	651	3.58
I am confident we deploy state-of-the-art access control technology given the level of control we need	10.49% 68	22.53% 146	18.83% 122	32.25% 209	15.90% 103	648	3.21

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q41 Please indicate how strongly you agree with each of the following statements.

Answered: 666 Skipped: 356

	STRONGLY DISAGREE	DISAGREE	COULD GO EITHER WAY	AGREE	STRONGLY AGREE	N/A	TOTAL	WEIGHTED AVERAGE
Upper-level management has an appreciation for the importance of access control	5.86% 39	13.53% 90	16.24% 108	36.69% 244	26.77% 178	0.90% 6	665	3.66
I am confident our staff knows what to do if they see someone they suspect should not be there	3.61% 24	9.34% 62	20.33% 135	42.32% 281	23.95% 159	0.45% 3	664	3.74
I am confident our staff knows and tries to follow all access control policies	3.31% 22	9.64% 64	18.07% 120	50.15% 333	18.07% 120	0.75% 5	664	3.71
When it comes to access control, my organization has done a good job of balancing employee convenience and providing security	4.80% 32	8.41% 56	18.17% 121	48.05% 320	19.07% 127	1.50% 10	666	3.69

ADDENDUM I: FULL SUMMARY SURVEY RESULTS

2023 Access Control Technology and Policy Study

Q42 If there is one thing you could change about your access control system or policies, what would it be?

Answered: 388 Skipped: 634

Various Open-Ended Answers