Excelling at Security Controls and Visibility

Benchmarking Research on the Approaches and Tools Deployed and How They Build Security's Value

ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

Sponsored by

FacilityOS

CONTENTS

ASIS International thanks FacilityOS for its sponsorship of this research. www.facilityos.com

INTRODUCTION AND KEY FINDINGS

Security controls are the resources, processes, and technology deployed to protect physical and information assets, and visibility ensures security controls are properly protecting assets as intended. Together, they are a bedrock foundation of security practice.

In partnership with sponsor FacilityOS, ASIS International Security Issues Research undertook a study to capture the current status and practice of security controls and visibility. ASIS fielded two surveys: One studying practices in place in corporate, educational, nonprofit, and governmental organizations, the other asking security consultants to assess the present state of controls and visibility. In some cases, results are compared to a similar survey conducted in 2023.

- Overall, organizations with good or excellent security controls and visibility experience fewer security incidents, are more prepared for emergencies, and have more support from other departments and top executives. (See pages 14-15.)
- Meeting the requirements of regulations, standards, or other compliance measures is an important security function utilizing security controls and visibility—78 percent of security professionals said their jobs involved compliance issues. (See pages 4-5.)
- When it comes to preventing unauthorized access, organizations are doing an excellent job overall. Sixty-five percent report that on average they have less than one unauthorized physical access incident requiring an action from security per week. (See page 6.)
- Technology used in access control systems has gotten more sophisticated since 2023. From use of smart RFID technology in cards and readers to biometric and mobile device controls, the use of more advanced access controls has increased dramatically since 2023. (See page 7.)
- The predominant methods used to deter or detect unauthorized access are security awareness training, actively monitored video, 24/7 guard patrols, and monitoring sensors and alarms. To protect primary entrances, surveillance again is the top method, followed by having guards stationed at entrances and ensuring open sightlines provide visibility to entrances. (See page 7.)
- Despite the success, security professionals see plenty of opportunities for improvement on such basic access control areas as piggybacking, propped doors, and false alarms. (See page 9.)
- Just more than half (55 percent) of security professionals say their organizations do a good job balancing employee convenience with security needs. The vast majority of the rest say their organizations are too concerned about convenience (38 percent) versus those who say their organizations are too concerned about security (7 percent). (See page 13.)
- Visitor and contractor management is often a complex visibility and control issue for security professionals. Nearly three-quarters say they would like to improve their capabilities in visitor management (72 percent) and contractor management (73 percent). (See pages 10-11.)
- Getting an accurate headcount of all people in a facility can be critical information in an emergency. However, 10 percent of security professionals are not at all confident they could get an accurate count, and another 22 percent were not very confident. Only 18 percent said they would be completely confident. (See page 12.)
- More than one-third of security professionals report their organizations do not have a set system or process to track high-value, potentially dangerous, or otherwise important inbound material packages or materials. Fully 71 percent of security professionals said they would like to see improvement in this area. (See page 8.)

SECURITY'S ROLE IN COMPLIANCE

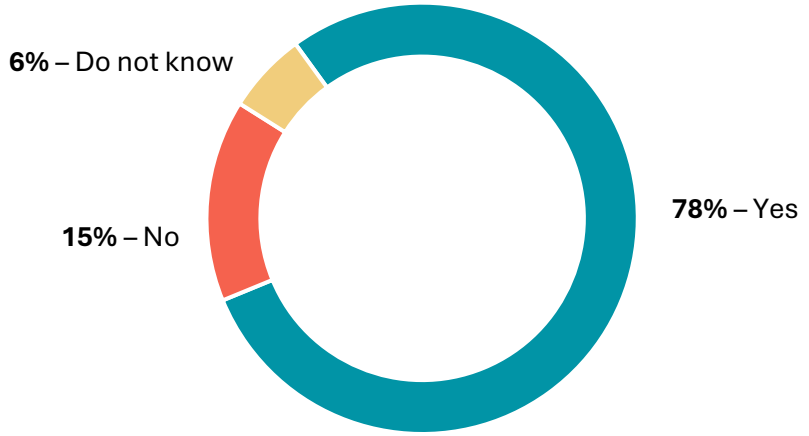
The ASIS International Physical Asset Protection Standard describes compliance as one of the fundamental needs of asset protection: "With input from asset owners, security professionals should establish, implement, and maintain procedures for periodically evaluating compliance with legal, regulatory, and other requirements."

Overall, more than three-quarters of security professionals said their organizations needed to meet security-related compliance objectives. Of those, the research asked a question designed to gauge the importance of compliance in their organization's security efforts. On one extreme, 27 percent said compliance is a primary way security adds value to the organization, and the largest segment (42 percent) said compliance was one of several important security responsibilities. On the other extreme, 13 percent said compliance was necessary, but security needed to focus on other, more strategic, areas.

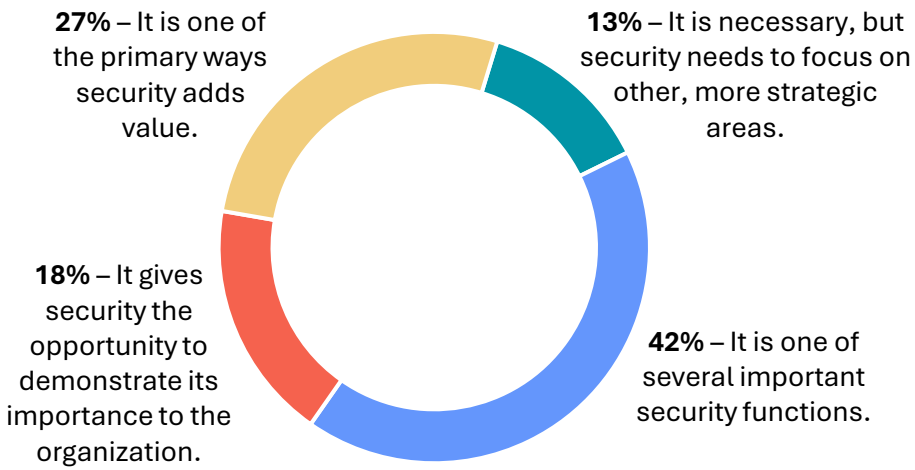
Security professionals were invited to list the three top laws, regulations, or standards affecting security. Researchers then assigned as many of these answers as possible to 1 of 10 categories. Of the more than 1,000 answers, 520 fit into one of the categories. (See table below.)

Type of regulation or standard	
Occupational safety & health, duty of care, workplace violence	28%
Cybersecurity or information security	15%
Security guard, private security, executive protection	14%
Supply chain and anti-terrorism	12%
Data privacy and consumer protection	9%
Identity, credential, or access management	6%
Critical infrastructure and energy regulations	6%
Defense, export control, and trade compliance	5%
Product safety, food defense, good manufacturing practices	4%
Quality and operational compliance	1%

Must security meet specific standards or requirements?



How do security's top leaders view security's compliance responsibility?



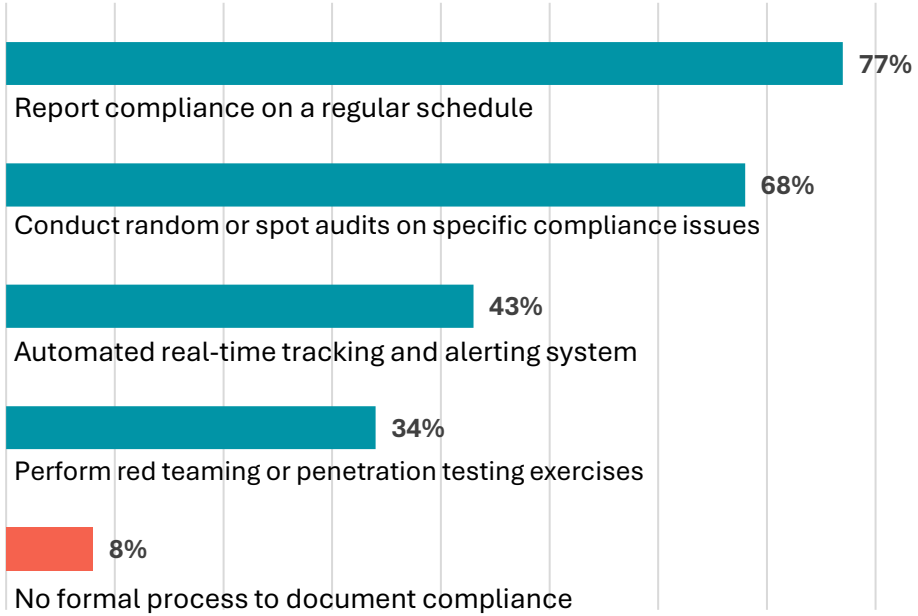
COMPLIANCE EFFORTS

Most organizations that count compliance as an important security function conduct random or spot audits on specific compliance issues and report compliance results on a regular schedule. However, less than half use an automated, real-time method to track compliance issues—and almost one-in-ten have no formal process for documentation.

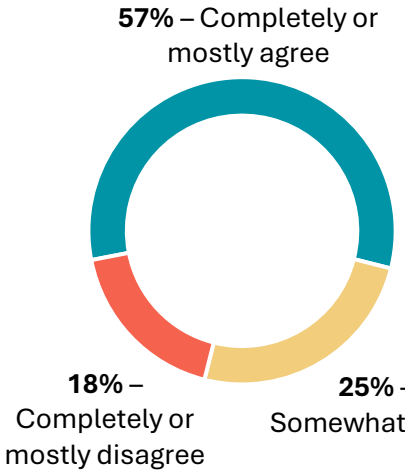
Consultants generally believe security leaders have a good understanding of the importance of compliance issues. However, fewer think organizations effectively audit and track compliance.

Overall, two-thirds of security professionals think their organizations put the right amount of effort into compliance, with the remainder split between too little and too much.

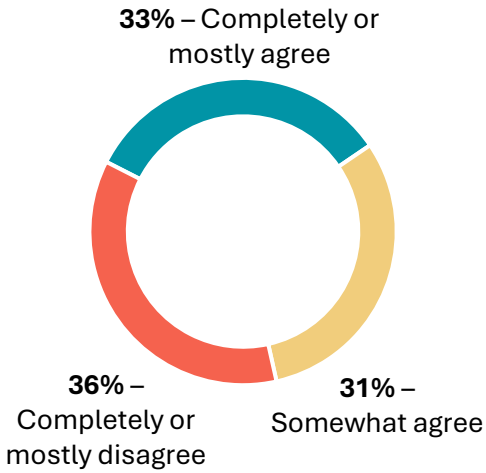
What actions do you take to ensure compliance?



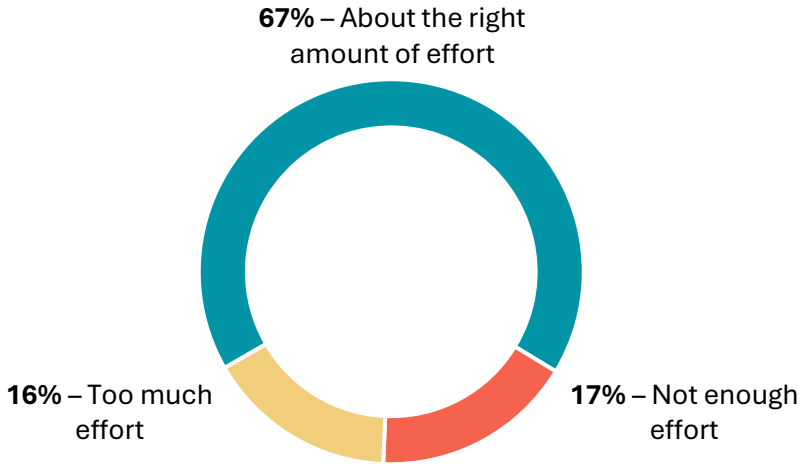
Consultants: Do security leaders have a good understanding of compliance importance?



Consultants: Are organizations effective at auditing and tracking compliance?



Does security put the right amount of effort into compliance?

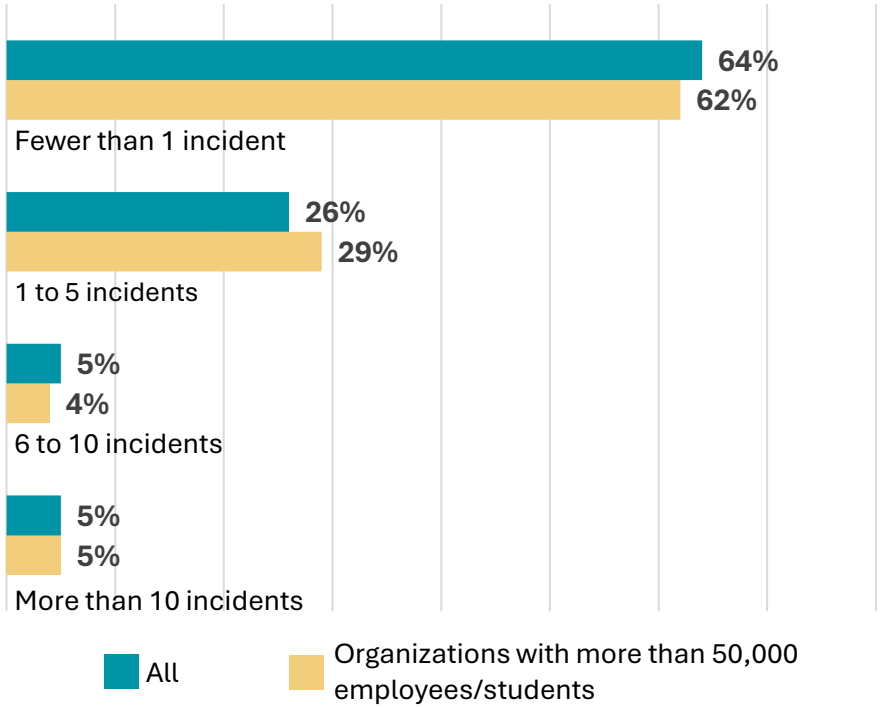


SECURITY CONTROLS ARE REMARKABLY EFFECTIVE

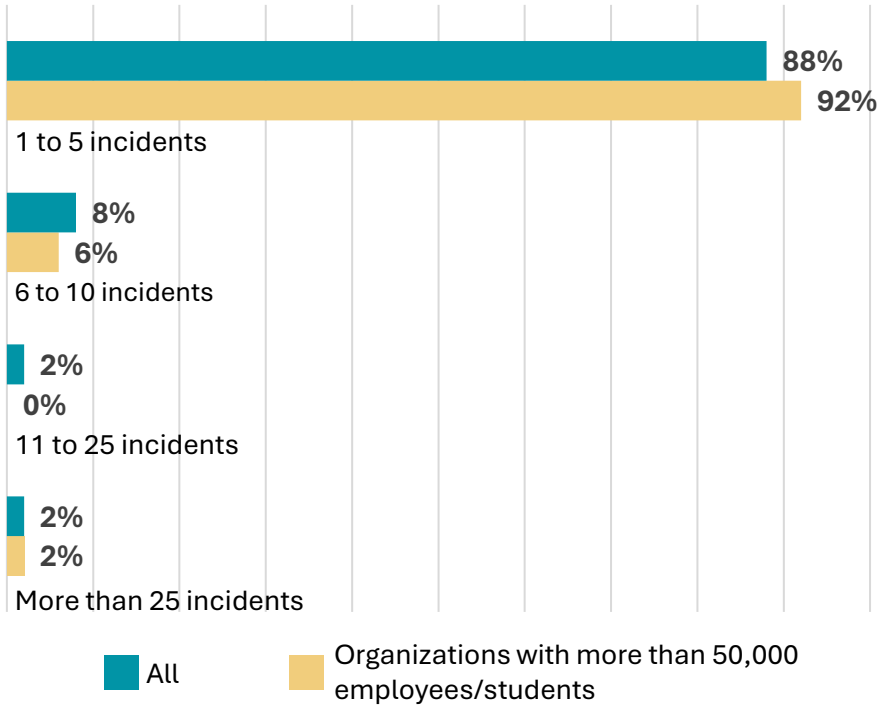
At least, they are effective when it comes to preventing unwanted access. Nearly two-thirds of security professionals reported they experience less than one security incident related to unauthorized physical access per week. The question itself defined "incident" as anything that requires security to take extra action to investigate or remediate.

Similarly, almost 9 in 10 reported that they had only one to five serious incidents related to unauthorized physical access per year. (The term "serious incident" was left to the participants to define for themselves.) In both cases, size had little to do with the number of incidents, even the largest organizations in the study had remarkably few incidents.

How many security incidents related to unauthorized physical access do you face per week on average?



On average, how many times a year does an unauthorized physical access incident result in a serious incident?

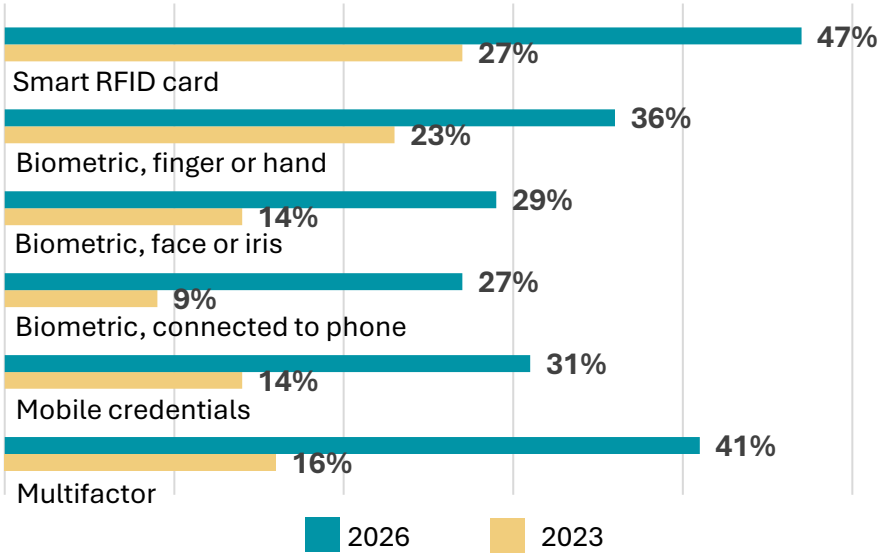


CONTROL TECHNOLOGY AND POLICIES IN PLACE

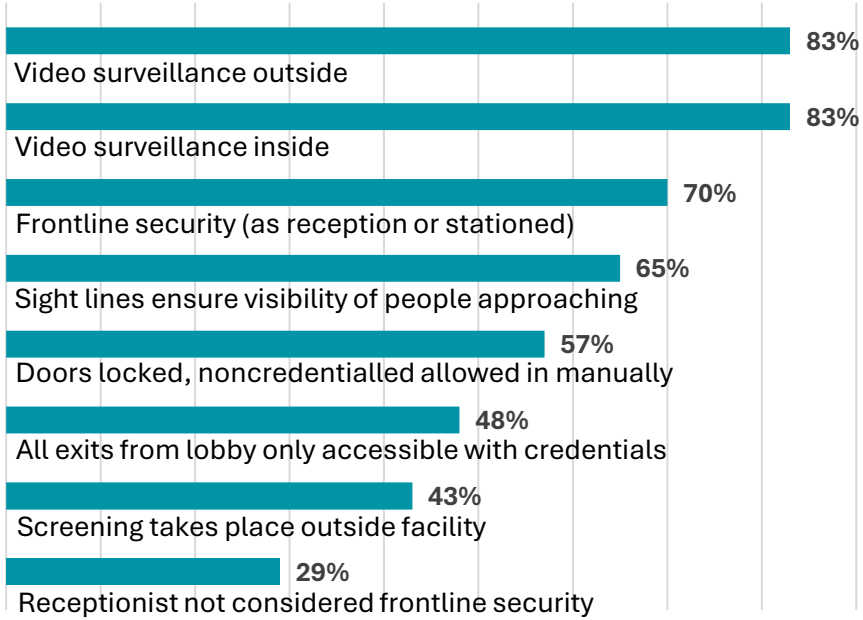
Organizations are adopting new access control technology at a significant pace. Smart RFID cards and readers are a more secure technology than traditional proximity cards, which can be easy to spoof. Smart RFID card use increased 20 percent compared to three years earlier and approached 50 percent. While use of biometrics, which are even harder to fake, lags smart RFID, all three kinds of biometrics studied increased in use by double digits.

Surveillance remains both a primary front entrance security fixture as well as a main method organizations use to detect access breaches. Guard patrols are, of course, another primary security measure, with 70 percent reporting they have guard patrols all day and night every day. It's also interesting that a bit under half (43 percent) of organizations screen people before they ever get to the main entrance.

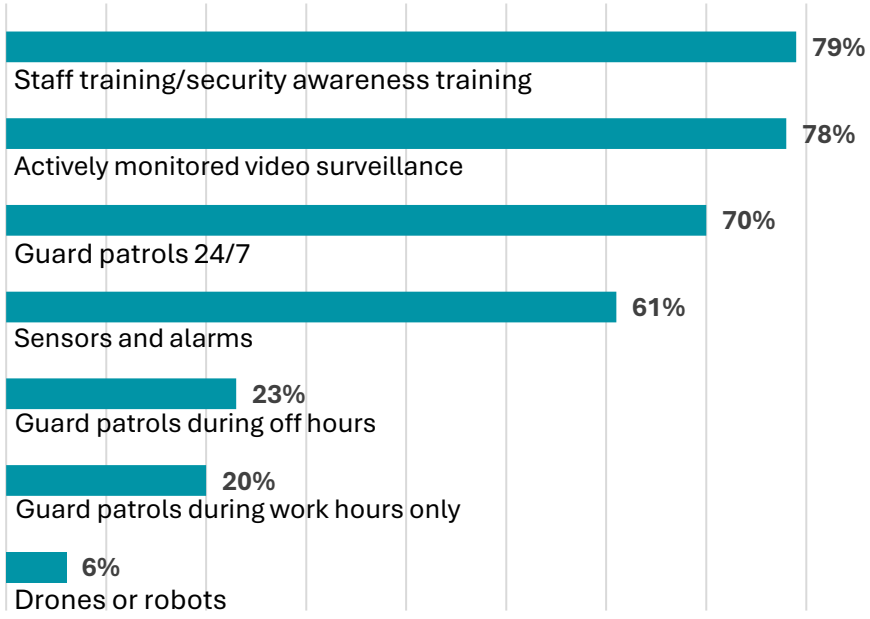
Which access control technologies do you use?



What security measures do you have at your main entrance?



How do you detect access breaches?



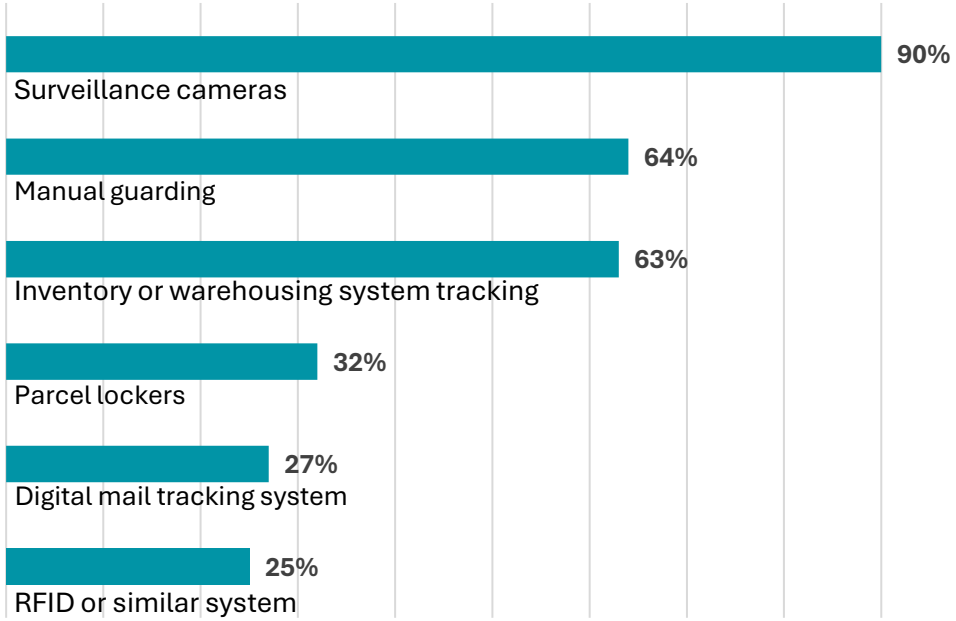
IN-BOUND MATERIAL SECURITY

Just under two-thirds of organizations have a system in place to ensure the safety and security of high-value, potentially dangerous, or otherwise important inbound material or packages.

Of those, most use a combination of surveillance cameras, manual guarding, and a dedicated inventory or warehouse management system to track the material or package. Fewer organizations use parcel lockers, digital mail tracking, or radio frequency ID systems.

Overall, 71 percent of security professionals said they would like to make improvements in this capability, and among consultants, only 33 percent said they thought organizations were entirely or mostly effective in this area.

What systems or procedures do you use to safeguard important material or packages?



Do you have a system in place to vet the safety and security of high-value, potentially dangerous, or otherwise important inbound material or packages?

71%

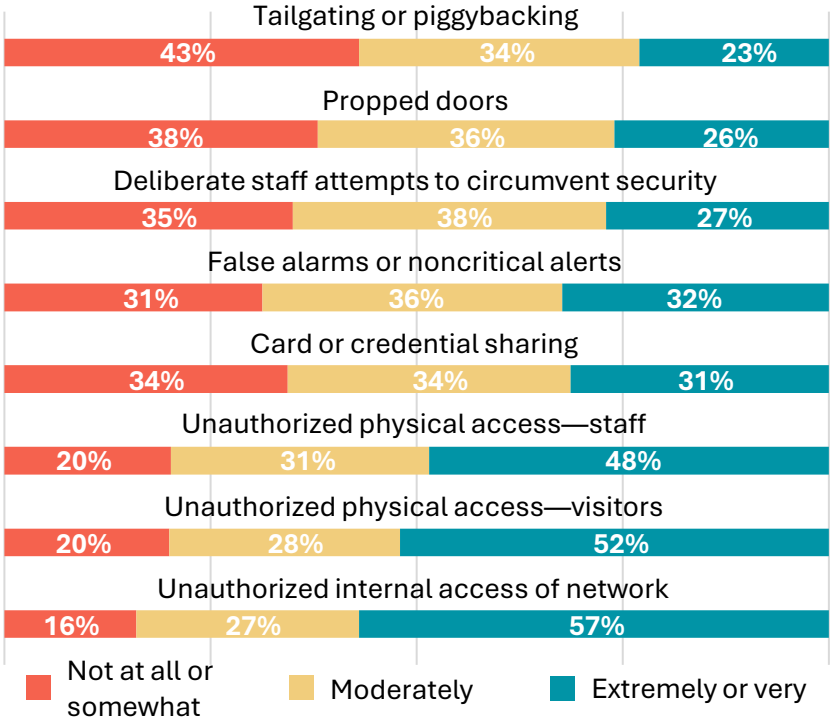
A total of 71 percent of security professionals said they would like to improve their ability to monitor or track important inbound material after it arrives at their facilities. Among consultants, two-thirds said organizations were only somewhat effective or worse at ensuring the safety and security of inbound materials and shipments.

COMMON SECURITY CONTROLS PITFALLS

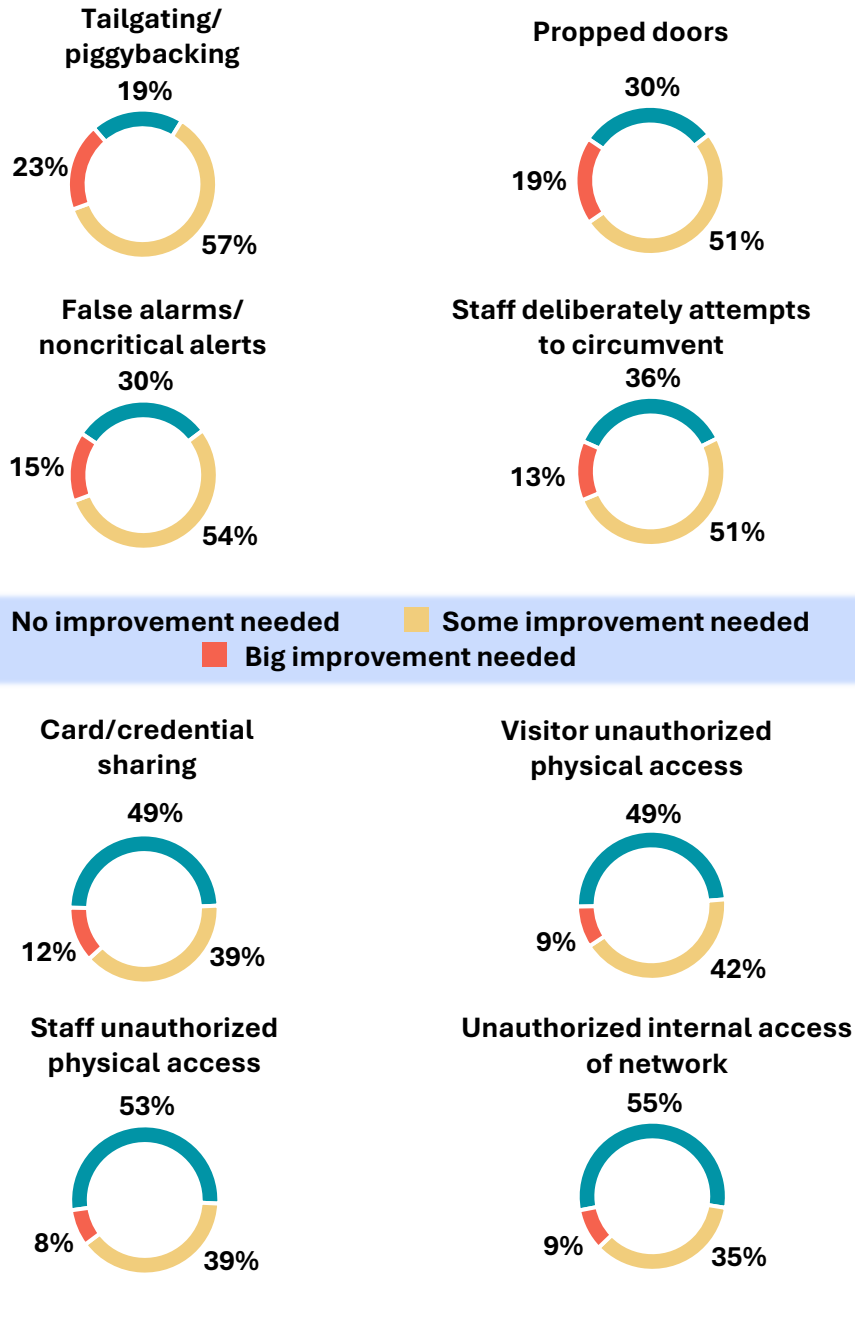
Despite the overall high performance in preventing incidents, security professionals reported plenty of areas that are ripe for improvement. The survey presented eight kinds of common security control evasions and asked them to choose if they needed to improve in that area. As the pie charts to the right demonstrate, a significant proportion of security professionals would like to see either some improvement or big improvement in all eight areas, with common security irritants—tailgating or piggybacking and propped doors—leading the way.

Consultants were asked to give their impressions on how well organizations performed across the same eight areas, and their answers mirrored the security professional results. The table below presents the consultant survey findings.

Consultants: How effective are organizations at preventing the following breaches?



Does your organization need to improve in these areas?



VISITOR MANAGEMENT

When it comes to security controls, visitor management is one of those perpetually difficult issues. Broadly, visitors include all nonstaff people accessing a site or facility. Their situations are highly variable from an outside sales rep coming for a one-hour meeting to an HVAC contractor that might be onsite all day or for a couple of days to a cleaning contractor that accesses a facility afterhours on an ongoing basis.

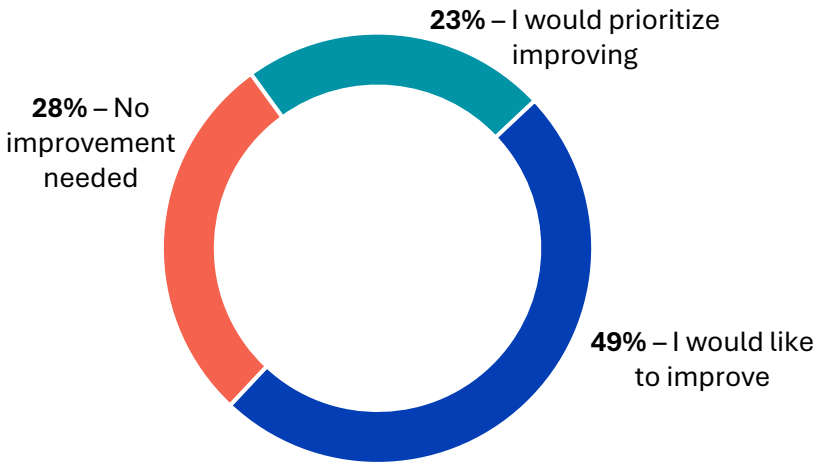
Almost three-quarters of security professionals (72 percent) say that they would like to improve their visitor management system. Overall, 60 percent have dedicated visitor management software. However, 23 percent use a pen and paper or simple spreadsheet to manage visitation, and 9 percent do not track visitor access.

The following page presents more details on visitor management practices. Most organizations have visitor processing times of five minutes or below, though 14 percent take longer, 5 percent do not track, and the rest say processing time varies depending on circumstances.

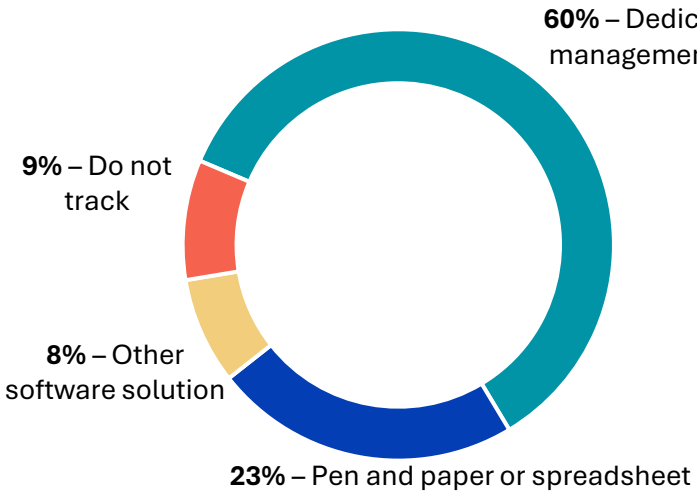
Approximately 20 percent of security professionals said they employed a digital watchlist screening procedure for all visitors. More common policies include requiring visitors to show a government-issued identification (74 percent) and requiring visitors to display a badge, sticker, or pin at all times (71 percent).

The survey also asked about tracking visitors once they are in a facility or onsite on a continuum of progressively tighter security control. The largest percentage said they knew all visitors in a facility, knew where they were in a facility, and knew when they left—41 percent. Another quarter (27 percent) said they knew entries and exits, but did not track them in a facility. In the loosest control scenario, 6 percent knew when some or most visitors entered, but not all of them all the time, and did not have a handle on when visitors departed. It's this last set of data that makes visitor management so vexing for organizations. Knowing who is in a facility and where is critical in an emergency. Survey results related to emergency management are on page 12.

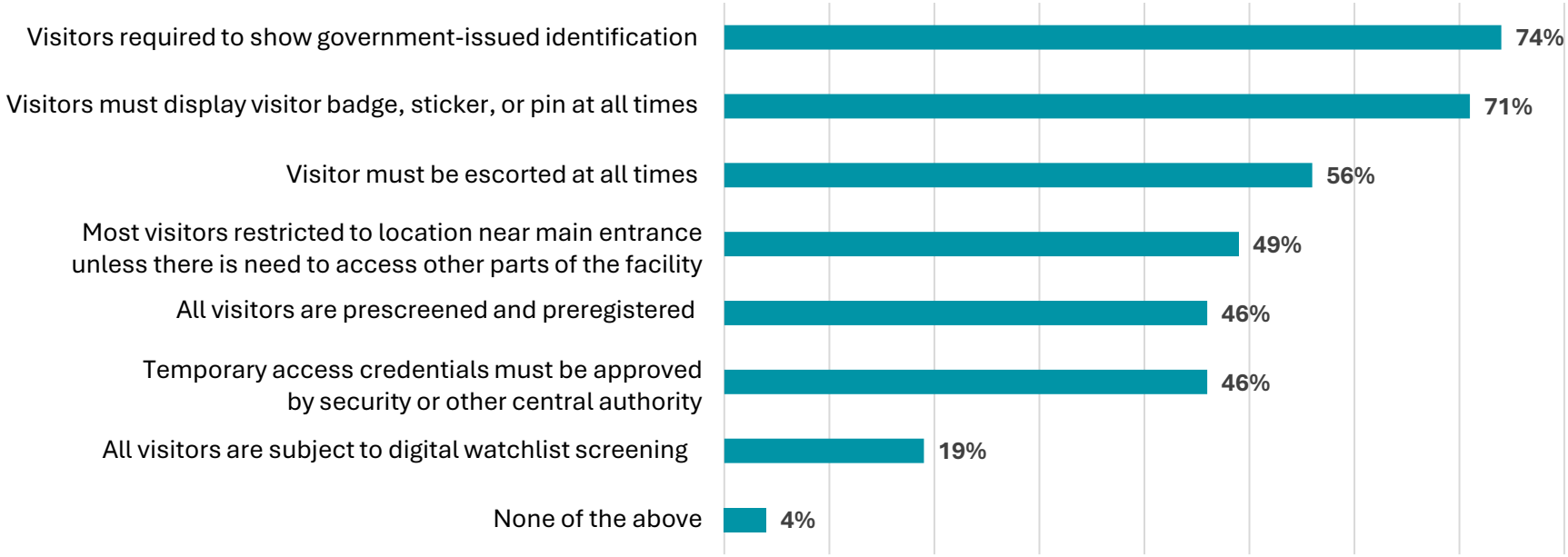
Would you like to improve how your organization handles visitor management?



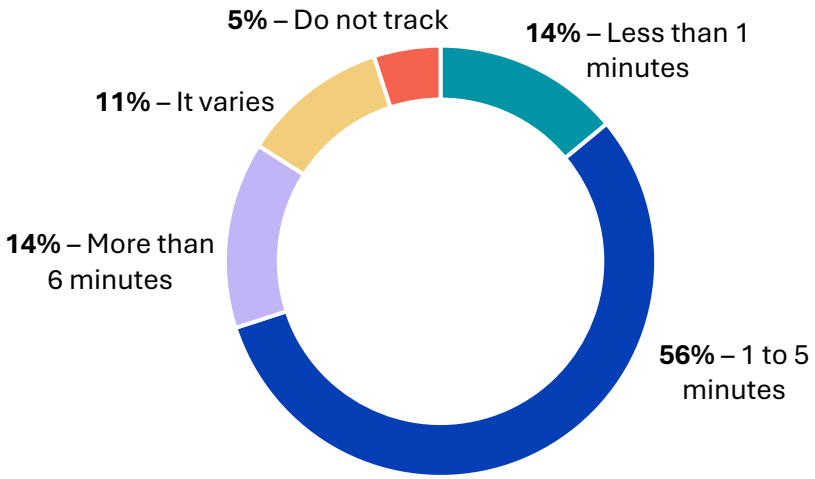
How do you track visitors in your facility? (If multiple facilities, answer for most advanced facility.)



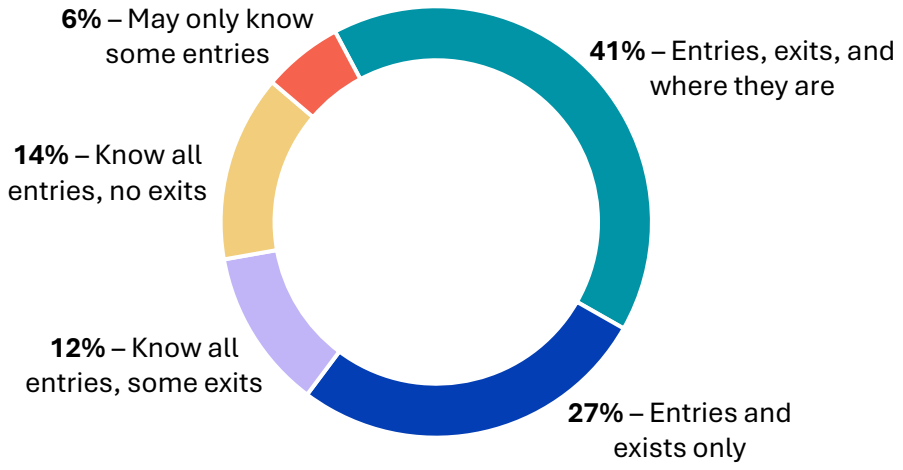
Which of the following visitor management policies or practices do you employ?



How long does it take you to process a temporary or short-term visitor?



How well do you track visitors in your facility? (If multiple facilities, answer for most advanced facility.)

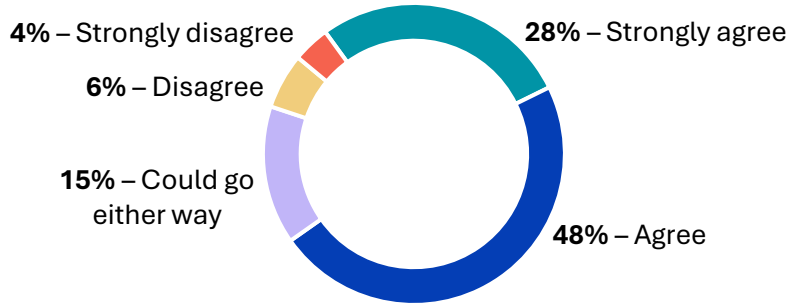


EMERGENCY MANAGEMENT

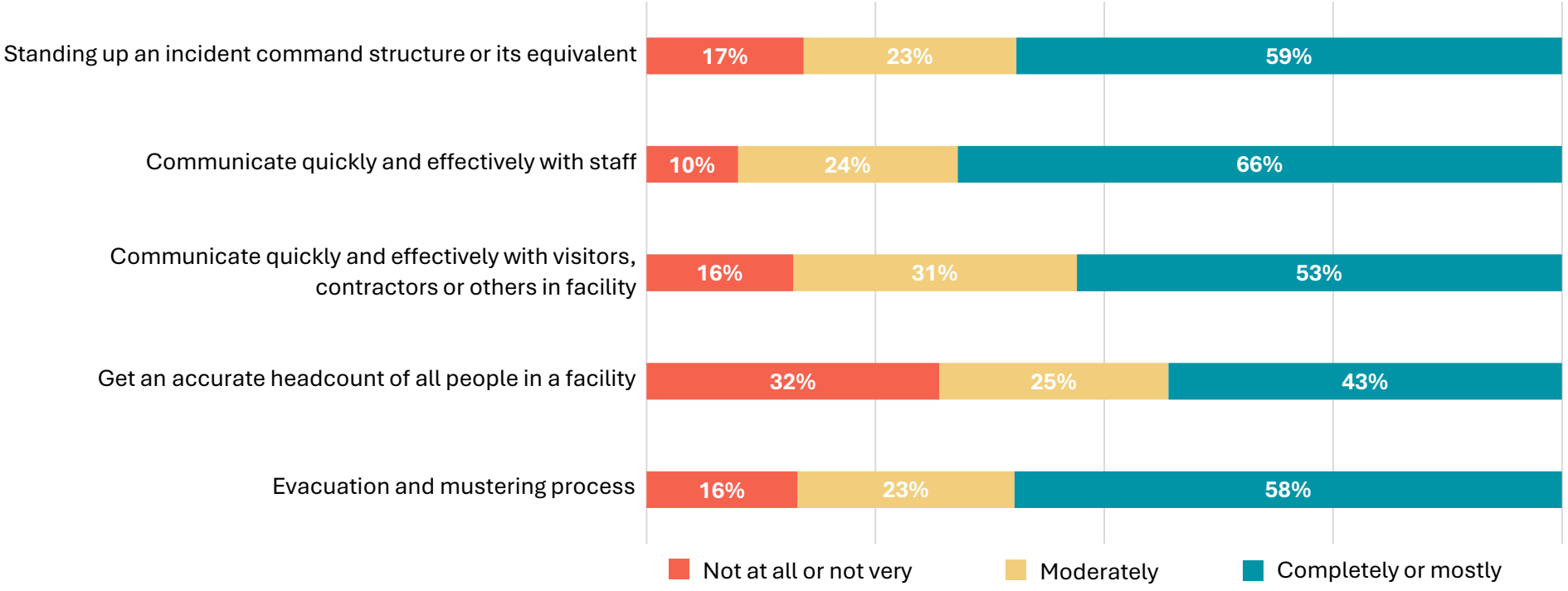
There are multiple reasons organizations need robust security controls and visibility. Pages four and five looked at a major one: being able to demonstrate compliance with regulations or standards. However, one of the most important reason is that control and visibility technologies and practices have a direct impact in major areas of emergency management. One-third (32 percent) of security professionals are not confident they could get an accurate headcount in an emergency, and another quarter are only moderately confident. Being able to effectively communicate with staff and visitors, and being able to effectively evacuate a facility, are derivative of knowing who is in a facility.

Page 15 shows that organizations with stronger visibility and controls are better prepared for emergency situations.

How confident are you that your organization is positioned as well as it can be to respond quickly and competently to an emergency situation?



How confident are you in your organization's capability in these emergency management areas?

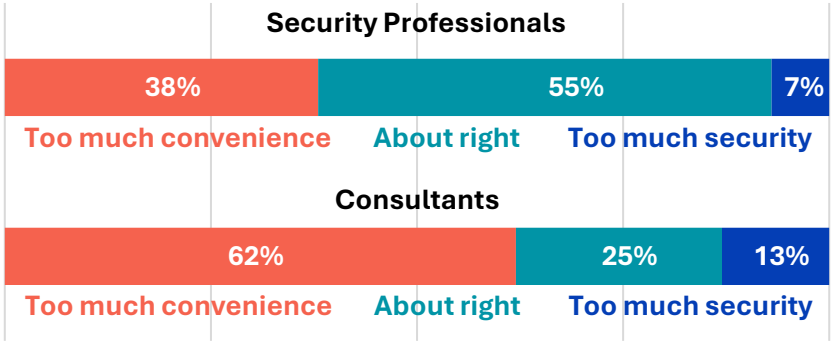


SECURITY CULTURE

A chart on page seven noted that the top method used to detect access breaches was security training which equates to having a security culture that encourages staff to report something if they see that it is amiss. It's also the best way to protect against four of the five most vulnerable access breach methods presented on page nine.

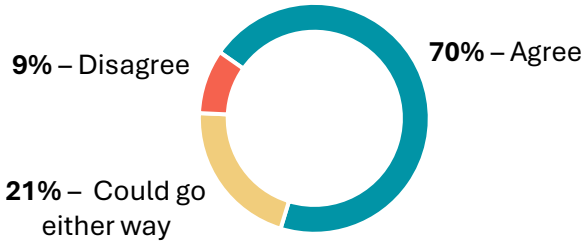
Creating a strong positive culture means finding the right balance between security controls needed and the inconveniences those security controls create—just over half of security professionals say they get the balance right, though the consultants surveyed weren't so sure. The pie charts below specific measure aspects of security culture.

How well does your organization balance security and employee convenience?

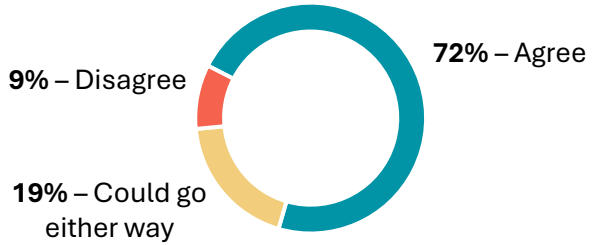


How strongly do you agree with each of these statements?

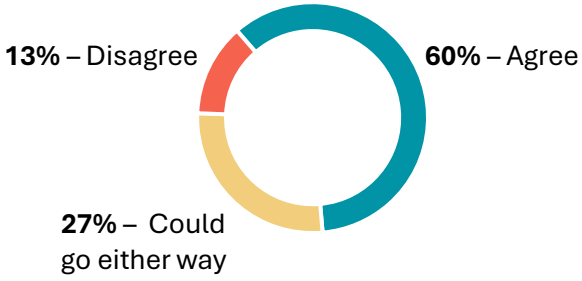
I am confident our staff knows what to do if they see someone they suspect should not be there.



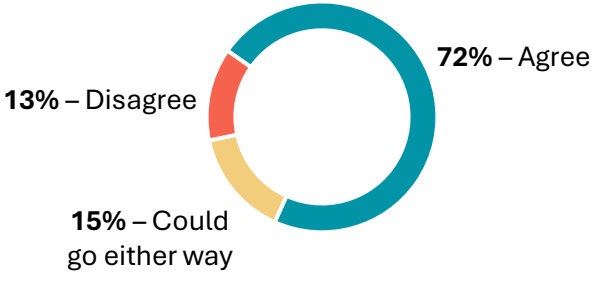
I am confident our staff knows and tries to follow data security and privacy policies.



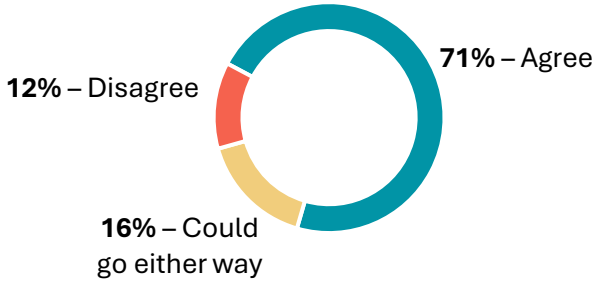
Other departments understand and support the organization's level of security.



Top executives have an appreciation for the importance of security controls.



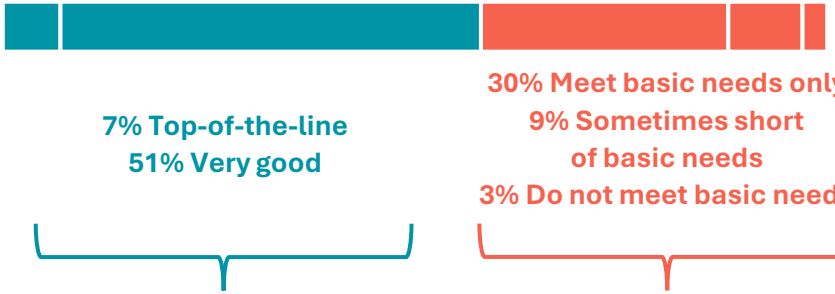
Top executives and the board understand and support the organization's level of security.



IMPORTANCE OF SECURITY CONTROLS AND VISIBILITY

The bar chart to the right depicts the results of a question that asked security professionals to rate the effectiveness of their security controls and visibility on a five-point scale. A bit over half said their controls and visibility was top-of-the-line or very good, and a bit under half said they "meet basic needs but nothing or very little more," or that they fell short of meeting basic needs some or all of the time. Dividing these into a "good" controls and visibility group and a "suboptimal" controls and visibility group, this enables this report to use crosstabulations to highlight the importance of controls and visibility across different factors. In every case the researchers examined, the good group had more desirable security outcomes than the suboptimal group. The bottom of this page and the next page highlight some of those areas having good security visibility controls affects.

Overall, how effective is your organization's security controls and visibility?



Security Incidents

How many security incidents related to unauthorized physical access do you face per week on average?

Good
69% – Less than 1 per week

31% – More than 1 per week

Suboptimal
57% – Less than 1 per week

43% – More than 1 per week

69% of organizations with good controls and visibility had less than one access incident requiring a security response per week compared to 57% for the suboptimal group

How many times a year does an unauthorized physical access incident result in a serious incident?

Good
91% – 1 to 5 incidents per year

9% – More than 6 per year

Suboptimal
82% –1 to 5 incidents per year

18% – More than 6 per year

91% of organizations with good controls and visibility had 1 to 5 serious incidents per year on average compared to 82% for the suboptimal group

Emergency Preparedness

Confident organization can stand up incident command structure

Good

77% – Completely or somewhat

23% – Not confident to somewhat confident

Suboptimal

36% – Completely or somewhat

64% – Not confident to somewhat confident

Organizations with good controls and visibility are much more likely to be prepared stand up an incident command structure in an emergency.

Confident organization is positioned to respond to emergency

Good

90% – agree or strongly agree

10% – Do not agree

Suboptimal

56% – agree or strongly agree

44% – Do not agree

Organizations with good controls and visibility are much more likely to be prepared for an emergency compared to those with suboptimal controls.

Security's Stature

Other departments understand and support level of security

Good

76% – Agree or strongly agree

24% – Do not agree

Suboptimal

38% – Agree or strongly agree

62% – Do not agree

Other departments are much more likely to support the level of security in organizations with good controls and visibility.

Top executives and board understand and support level of security

Good

84% – Agree or strongly agree

16% – Do not agree

Suboptimal

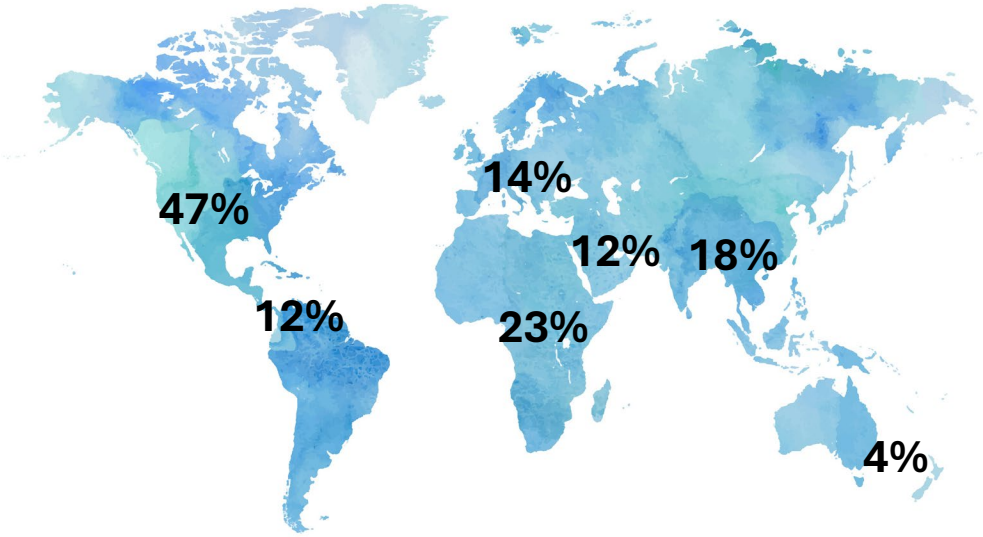
53% – Agree or strongly agree

47% – Do not agree

Top executives and the board are much more likely to support the level of security in organizations with good controls and visibility.

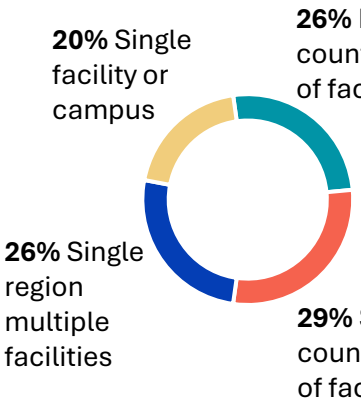
DEMOGRAPHICS

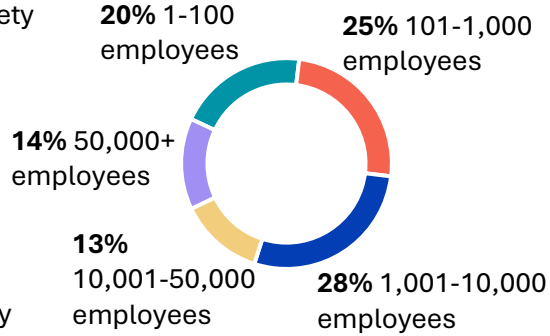
Survey Demographics: Geographic Scope



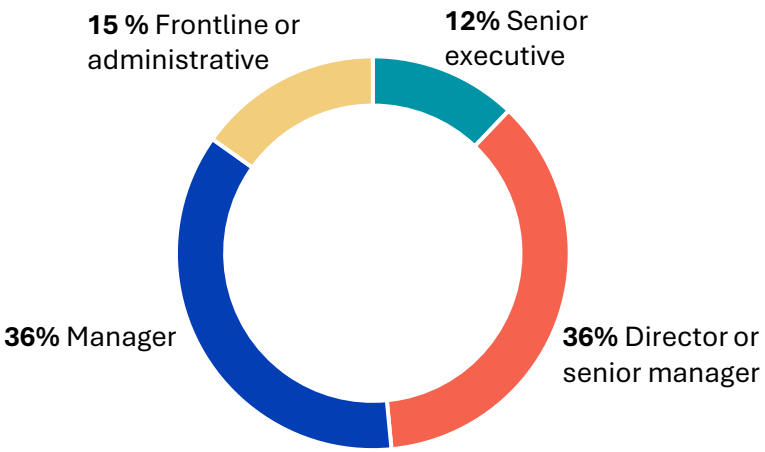
Participants were instructed to select all regions for which they had responsibility.

Organization Size and Scope





Position



Sector	
Banking, Finance, and Insurance	8%
Manufacturing	7%
Defense and Intelligence	6%
Oil, Gas, and Chemical	6%
IT and Telecommunications	6%
Government (other than defense, law enforcement, or education)	5%
16 others less than 5% each	62%

METHODOLOGY

In the second quarter of 2026, ASIS International convened a small group of ASIS members and a representative from project sponsor FacilityOS. This group put together a survey which was fielded in the month of May. The survey was promoted to ASIS members and customers via email, social channels, and ASIS newsletters. A total of 942 people answered at least some questions. All responses were recorded and used in this analysis regardless of whether the participant completed the survey. Security consultants and service providers were given the option to take an alternate set of questions. In total 637 people answered the last question available to them in the survey, which includes 131 consultant surveys and 506 standard surveys. Note: Some figures in the charts and tables that should add to 100 percent do not because of rounding.

The margin of error for most questions in the standard survey is plus or minus 4 percent at the 95 percent confidence level. The margin of error for the consultant survey is plus or minus 9 percent, so the consultant results should be taken as a guide rather than as statistically significant research.

One source of bias could be that the survey was promoted as a security controls and visibility survey. People who self-select to take such a survey could reasonably be considered more knowledgeable about the topic than other security professionals and organization leaders and perhaps more advanced in their practice. In addition, while the survey did not ask them to identify themselves, it is likely that a significant majority of the survey participants are ASIS members. This could also introduce bias because, similar to those who would self-select to take a survey based on its topic, ASIS is an organization dedicated to promoting best and promising practices in corporate security, and its members may have a more advanced knowledge of security concepts than nonmember security professionals.

Project leader:
Scott Briscoe
Content Development Director, ASIS International
scott.briscoe@asisonline.org

ABOUT THE SPONSOR

FacilityOS is a global leader in facility, asset, and visitor management. The integrated platform gives security and facility teams full control and visibility over who is on site, at every entry point and every moment. It automates the processes that matter most for security: visitor check-in, identity verification, credential issuance, access permissions, and compliance reporting, all from one centralized platform. FacilityOS enforces safety protocols and site security requirements while helping organizations meet regulatory compliance standards, replacing manual, disconnected processes with a single source of truth for who is on site and why. Trusted by 30% of the Fortune 500, FacilityOS gives security leaders the real-time visibility and operational control they need to protect people, assets, and facilities across every location.

FacilityOS