ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

ACTIVE ASSAILANT PREPAREDNESS:

RISKS AND RECOMMENDATIONS

Sponsored by

everbridge™

CONTENTS

KEY FINDINGS

ASIS International, with partner Everbridge, has been studying trends in active assailant readiness and response for several years. The 2024 Active Assailant Preparedness Survey repeated several benchmarking questions with previous surveys in order to uncover how approaches have evolved while examining several new areas critical to understanding the current state of active assailant preparedness.

ASIS fielded the survey in June and July 2024, resulting in 700 responses. ASIS staff then led conversations with subject matter experts to gain context and understanding on the results. The following are the key takeaways from the research.

1 Violent acts may have declined slightly, but active assailant preparedness and workplace violence prevention remain key security concerns.

Both the 2023 and 2024 surveys asked security professionals if they had experienced any of several different violent incidents in the previous five years, from workplace violence that required ambulatory assistance to someone brandishing a deadly weapon to a bomb threat they believed potentially credible. For each type of incident, there were small, but statistically significant, declines in 2024 compared to 2023. However, both years had the same top security concerns: active assailants, workplace violence, and cybercrime—though the rank order of those concerns changed from year to year.

2 Anticipated time to respond to an incident has improved slightly, though communication during an incident is still a top issue.

In an active assailant situation, quick communication saves lives. In 2024, 23 percent of security professionals said it would only take seconds for their employees or students to be notified of an active shooter incident. That is a small, but statistically significant increase compared to 2023's 16 percent. In 2024, communicating with people in a building or campus ranked second on a list of concerns security professionals said they would have in an active assailant incident with 46 percent. Other communications concerns also rated highly, including the most-cited concern: getting real-time updates as the situation unfolded (50 percent).

3 An increase in hybrid work environments has not decreased the need to prioritize workplace violence issues.

The pandemic changed the circumstances for many of the participants in the 2024 survey. Nearly half said they implemented a hybrid work schedule and 35 percent reported they have substantially more remote workers. Just under 3 in 10 said there was little change in where people worked. However, 55 percent of security professionals said their approach to active assailant preparedness has not changed. Only 8 percent report it has become less of a priority.

4 Training and using threat assessment teams are common active assailant preparedness measures.

Two-thirds of security professionals report active assailant training or education for employees or students is an important countermeasure, and three-quarters have trained using the run-hide-fight protocol (or variants, such as avoid-deny-defend). Two-thirds of security professionals also report having a threat assessment team that evaluates potential active assailant threats.

5 Despite the preparation, there is still a lot of doubt from security professionals about how prepared their organization is for an active assailant incident.

The survey asked security professionals to rate how confident they were that their organizations were

prepared for an active assailant incident, from not-at-all confident to highly confident. More of them chose not-at-all confident than highly confident, and a total of 63 percent had a medium level of confidence or lower.

6 **Factors that make a difference in that confidence level: having a specific plan in place, investing in communications, training staff or students, and deploying threat assessment teams.**

These are all considered best practices and are detailed in the Active Assailant annex to the ASIS Workplace Violence and Active Assailant Prevention, Intervention, and Response Standard, so it is no surprise that these practices affect active assailant preparedness. However, the differences uncovered in the study are truly astounding. Using planning as the example, having a plan in place results in 56 percent of security professionals being mostly or highly confident that their organizations are prepared for an active assailant. That compares to just 9 percent of security professionals whose organizations do not have a plan in place. Similar differences run across all four factors.

UNDERSTANDING THE IMPORTANCE OF ACTIVE ASSAILANT PREPAREDNESS

The chances of a multi-casualty incident occurring at any particular place are very small. But the chances are not zero, and if it does occur the impact on businesses and communities involved is extreme. Preparation for active assailants is essential. Most importantly, preparation can lead to prevention, which is the ultimate goal. However, if an active assailant incident does materialize, preparation also saves lives and enhances the recovery process.

The threat of an active assailant has long been at or near the top of the list of potential threats security professionals say they must prepare for. In 2024, the more general threat of workplace violence topped the list, with 49 percent of security professionals listing it as one of their top three security threats. Active shooter, which is an extreme act of workplace violence, was selected as a priority by 42 percent of security professionals, just behind cybercrime, which was at 44 percent. Theft of physical property came in fourth, cited by 33 percent of security professionals.

ASIS and Everbridge asked the exact same question in surveys in early 2023 and in 2020. In all three studies, those four security threats topped the lists, though the orders and percentages changed some from year to year (see Figure 1.1).

Figure 1.1: Most Important Security Threats

2024	2023	2020
Workplace Violence 49%	Active shooter 51%	Active shooter 48%
Cybercrime 44%	Workplace Violence 47%	Cybercrime 48%
Active shooter 42%	Theft of physical property 40%	Workplace Violence 42%
Theft of physical property 33%	Cybercrime 38%	Theft of physical property 35%

Figure 1.2: Violent Incident Occurred at Organization in the Last Five Years

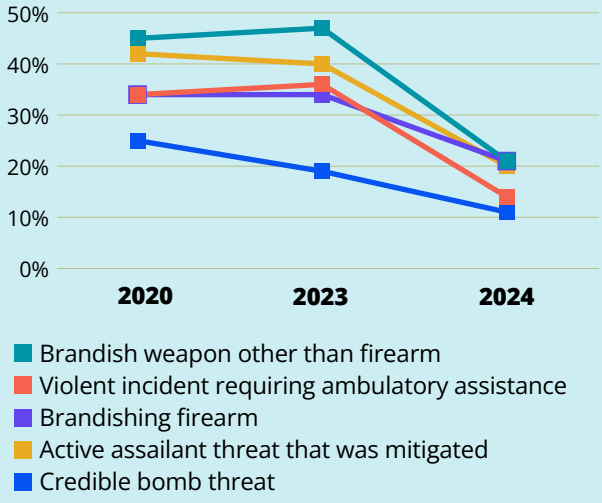
The 2024 survey presented six different acts of violence and asked security professionals if their organization experienced any of them in the previous five years, or for as long as they've been at the organization if that is less than five years. Just more than half (51 percent) said they had not faced any of the seven. Eight percent reported they had experienced a workplace violence incident that resulted in a fatality, and 14 percent experienced a violent incident that required ambulatory assistance or hospitalization (see Figure 1.2).

In a positive development, violent incidents declined slightly when comparing 2024 to previous years. The surveys asked the same question from year to year, however, some of the answer choices in 2024 were different. Most did not change, or did not change substantially, however, and those that did not change showed consistent decreases. Violent incidents requiring ambulatory assistance were experienced by 36 percent of security professionals in 2023, that is 22 percent more than in 2024.

Likewise, brandishing a firearm (13 percent decline from 2023 to 2024), brandishing a different kind of deadly weapon (26 percent decline), and credible bomb threats (8 percent decline) all were cited by fewer security professionals (see Figure 1.3).

Despite these decreases, another indication that the active assailant threat remains a top concern is that a majority of survey participants said executives at their organization were more concerned about employee or student safety now than they were two years ago. Each year of the survey has returned a similar result.

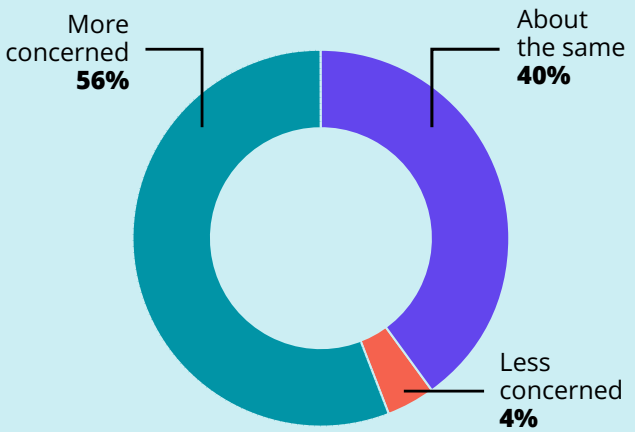
Figure 1.3: Violent Incident Trends



Percent of participants that said incident had happened at their organization within the past five years.

Researchers asked security professionals if their organizations' executives and security decision makers were more or less concerned about employee or student safety than they were two years ago (see Figure 1.4). From 2020 to 2023 and now 2024, the results were incredibly similar to each other, with a solid majority saying their executives were more concerned, with most of the rest saying the concern level had remained about the same. The threat landscape organizations face continues to evolve and grow in complexity, but these findings underscore that the active assailant threat continues to demand attention.

Figure 1.4: Are Executives More or Less Concerned About Employee or Student Safety?



COMMUNICATION IS PRIMARY CONCERN

There really aren't any endeavors at organizations that do not require strong communication, and that's certainly true of anything the security department hopes to accomplish. If there is a time when it is most important, though, it just might be during an active assailant incident. Speed and accuracy of communication at such a time can be the difference between life and death.

Communication is certainly important in preventing active assailant incidents. How many mass casualty post incident analyses highlight communications shortcomings? If only the right message had reached the right recipient, a tragedy might have been avoided.

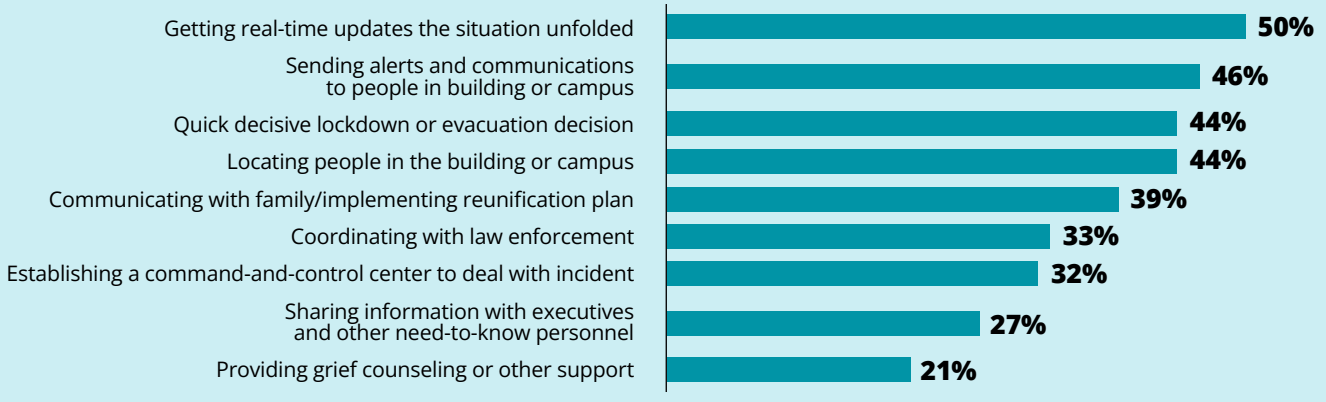
And when an active assailant incident is unfolding, chaos reigns. Organizations that have prioritized and practiced quick, accurate, and continued communication will have a much better opportunity to contain and neutralize the assailant and move to recovery smoothly and quickly.

The survey asked security professionals what their biggest challenges would be if an active assailant incident were occurring at their organization. Issues related to communication comprise the top three challenges. The biggest challenge was getting real-time updates as the situation unfolds, cited by half of security professionals. The next biggest challenge, cited by 46 percent, was sending alerts and communications to people in the building or campus affected. Making a quick, decisive lockdown or evacuation decision—which is a communications issue—came in at 44 percent. (See Figure 2.1 for the full list of challenges.)

Drew Neckar, CPP, principal consultant at COSECURE, said, "It's critical that the people who are responsible for sending that lockdown communication know and understand their role." He said too often, organizations have not established clear processes. He related the time he was working with university, and the leaders said it was the police dispatcher who was responsible for sending an alert. When he asked the dispatcher, the dispatcher told him he knew they had the system, but he wouldn't feel comfortable using it without the chief's approval. "That's a system that doesn't work at 3 a.m.," Neckar observed.

Meeting these communications challenges means planning. Fortunately, a robust 73 percent of security professionals say their organization has a communications plan in place for active assailant incidents, so at a minimum there is a foundation around which to work on making improvements.

Figure 2.1: Biggest Challenge During an Active Assailant Incident



"Looking at the early results of the survey, I thought it showed a lot of good things, that a lot of people are taking these issues and these threats seriously and taking actions to protect their organizations," said Gene Petrino, a security consultant with Survival Response LLC.

The survey examined the second-biggest challenge—sending alerts and communications to people in the building or campus—in greater detail. Nearly 7 in 10 security professionals said they had deployed a technology solution to enable communications to impacted constituents in the event of an active assailant (see Figure 2.2). Another 15 percent said they planned to invest in such technology.

"The early notification systems are absolutely critical," Petrino said "They work incredibly well, and they are absolutely critical to reducing casualties and increasing apprehensions."

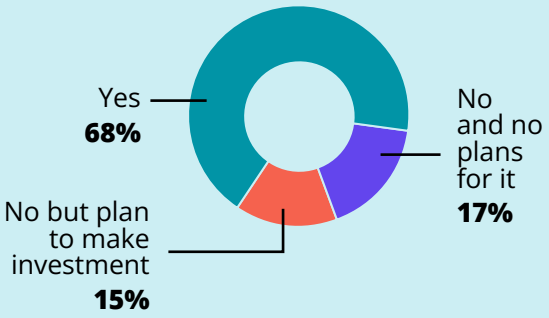
When asked how long it would take to notify constituents of an incident, most security professionals said it would take minutes. Less than one-quarter said they could get an alert or communication out in seconds (see Figure 2.2). For both of these findings—having a technology solution and the length of time it would take—findings did not differ appreciably from 2023 or 2020, denoting that progress is not being made in this all-important area.

Finally, researchers asked how often organizations conduct drills of their system for alerting constituents during an emergency. One-quarter drill once per year on average, 4 in 10 do so more often than that, and the rest either do not drill regularly or do not have a system in place (see Figure 2.2).

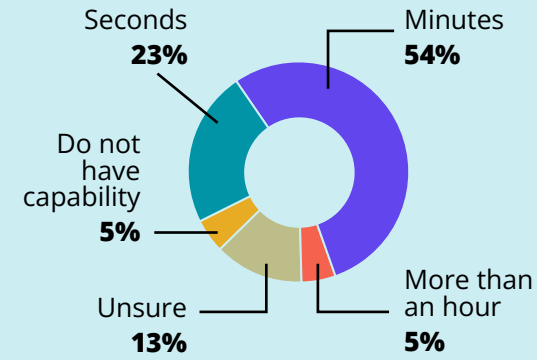
"As good as the systems are," Petrino continued, "you have to have a good process in place for using it. It can't just be one person, but it also can't be 15 people. And testing it is absolutely important."

Figure 2.2: Alerting Constituents to an Active Assailant Situation

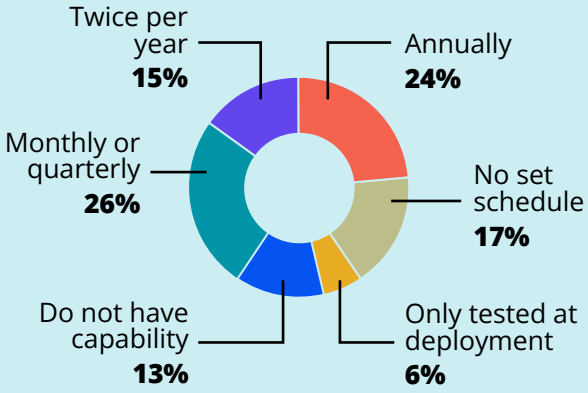
Have a Technology Solution for Alerting Constituents



Time It Would Take to Notify Constituents



Frequency of Emergency Notification System Testing

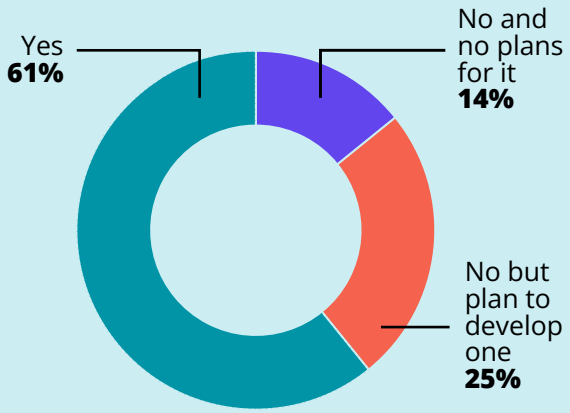


MEASURES TO TAKE BEYOND COMMUNICATION

There is more to active assailant preparedness than ensuring communication channels are in order. Specifically, organizations must have a workplace violence prevention plan that includes prevention and preparation measures for the most severe workplace violence incident: an active assailant situation.

A little under two-thirds of security professionals said their organization has a comprehensive response plan in place for active assailant incidents. Another one-quarter said they have plans to implement such a plan (see Figure 3.1).

Figure 3.1: Have a Comprehensive Response Plan for Active Assailant Incidents



A comprehensive rubric for creating such a plan is detailed in the ASIS Workplace Violence and Active Assailant Prevention, Intervention, and Response Standard. As noted, while the likelihood of an active assailant incident is low, it does not take much imagination to understand how destructive such an event can be or why it needs to be avoided if possible and palliated if one does occur. And despite it being a top security concern, nearly 40 percent of organizations do not have a comprehensive response plan in place. Why?

One answer may be security's role and influence in organizations.

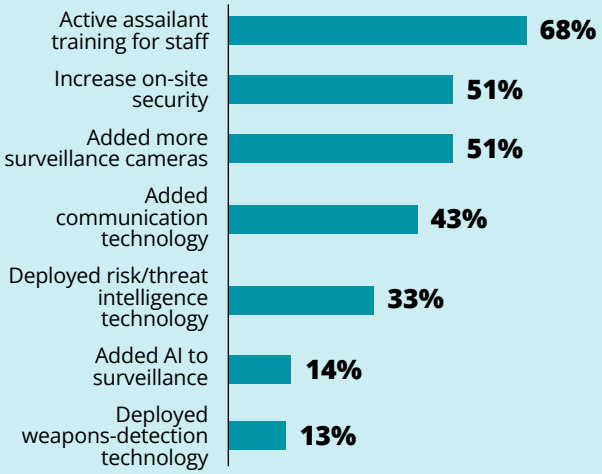
"A lot of times, in a lot of organizations, the security director may not have the power to focus on this issue the way they would like," Petrino said. "If the CEO or the decision makers do not see the value of it, will not be convinced it is necessary, then the security director is left to do what they can with the means that they have."

Security's influence in organizational risk management has been the subject of two recent ASIS research projects: The Current State of Security Risk Management: Benchmarks and Effectiveness Measures and the ASIS Foundation's The Influence of Security Risk Management. These reports measure the influence security professionals have and examine methods security professionals can employ to increase that influence.

The survey asked security professionals what steps they had taken to improve their active assailant or workplace violence preparedness. Active assailant incident training with employees led the way, with two-thirds of security professionals saying their organization had taken the action (see Figure 3.2). Organizations also added surveillance cameras (51 percent), increased on-site security (51 percent), and invested in communications technology (43 percent). Fewer organizations had added artificial intelligence to surveillance (14 percent) or deployed weapons-detection technology (13 percent).

In addition to the closer examination of communications practices and technology detailed in a previous section, researchers also asked several questions

Figure 3.2: Actions Taken to Improve Active Assailant Preparedness



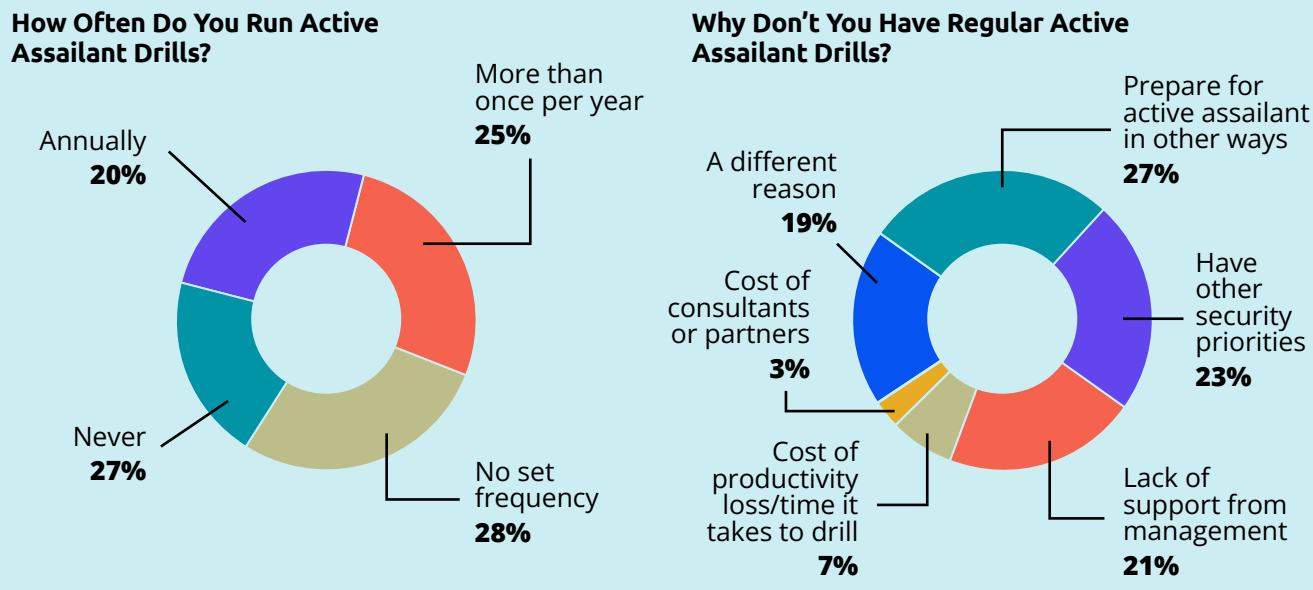
on both active assailant training and use of threat assessment teams. In addition to the closer examination of communications practices and technology detailed in a previous section, researchers also asked several questions on both active assailant training and use of threat assessment teams.

As Figure 3.2 shows, 68 percent of organizations train staff to prepare for an active assailant incident. The survey asked how often organizations run active assailant drills (see Figure 3.3). The term "drills" was not defined, and participants could have interpreted it to mean a company-wide simulation or training event, a tabletop exercise with security and other accountable areas, or anything in between. Overall, a quarter of participants reported their organizations never run active assailant drills and another quarter said they run drills but with no set frequency. The other half run drills regularly, with an annual drill (19 percent) being most common.

Those who do not run drills regularly were then asked for the primary reason why. The most common reasons were that they prepare for active assailant situations in other ways (27 percent) followed by other security priorities taking precedence (23 percent).

Finally, researchers asked specifically about the run-hide-fight protocol, or its variants, such as avoid-deny-defend: 77 percent said their organizations used run-hide-fight or similar protocols in training staff.

Figure 3.3: Active Assailant Training



"I'm not a huge advocate of live training drills," said Petrino. "I think the real value is in tabletops and individual employee training in aspects of it," noting that the run-hide-fight training is the type of aspect training that can be important when done well.

While the survey focused on training specific to active assailant incidents, it is important to note that general security awareness training is incredibly important for working to prevent an incident from occurring in the first place.

"Take a mid-sized hospital," Neckar said. "It may have 30 to 40 security employees, but it will have four to five thousand other employees. Security's eyes, even with cameras and sensors, cannot be everywhere at once. So equipping people with the idea of knowing what is suspicious, and then knowing what to do with that information is incredibly important."

Petrino told a story of showing up 30 minutes early for a consulting meeting in a city. He said it was a busy area, but not super busy, and he and his colleague got out of their car and were talking in the parking lot. Someone came by and asked, in a friendly way, if he could help them. They explained they were early for an appointment, and the man said he would let the person know we were there. About five minutes later, someone walking out of the building saw them and came over to them and it was the same thing. Just as they were getting ready to walk in for the scheduled meeting, a janitor was outside collecting trash and did the same thing, and then offered to walk them in and get the security director. "None of these people were security officers, and they had security officers. That is what proper training looks like."

Standing up a threat assessment team is another tactic commonly referenced as a best practice when it comes to workplace violence prevention. Like security awareness training, the purpose of deploying a threat assessment team is to prevent violent incidents. In fact, done correctly, threat assessment teams factor significantly into security awareness.

"You want your employees to know the difference between someone getting angry and punching someone in the nose and someone who feels they have a grievance, someone who may be making preparations for violence that they may act on," Neckar said. "You're looking for changes to baseline behaviors and signs of escalation. And your employees need to who to report this to and how to report it."

Overall, nearly one-third of organizations have a threat assessment team that evaluates potential active assailant threats and works to intercede to prevent them (see Figure 3.4). Of those who make use of threat assessment teams, 39 percent reported the teams were primarily a security department function—a less than ideal situation.

"A lot of times you'll talk to people about threat assessment teams and they say that's a security issue, and it should be security doing the work," Petrino said. "I think that's a mistake. I think you want to have someone from HR involved and you should probably have someone from legal. You won't to get the whole picture, and you need different views and different perspectives to investigate and analyze potential threats."

More than half of the security professionals in the survey (56 percent) described their threat assessment in similar terms: as a cross-functional team that spanned multiple departments. The other five percent said threat assessment teams were primarily the responsibility of human resources or legal teams rather than security or a department-spanning team.

The time and resource investment in threat assessment teams paid off for many organizations: 42 percent of security professionals in organizations with the teams said the team took an action or instigated an intervention that saved the organization from a serious workplace violence incident (see Figure 3.4). Further confirmation: after-incident analysis often reveals signs or clues that if they had been acted upon organizations may have prevented an act of violence.

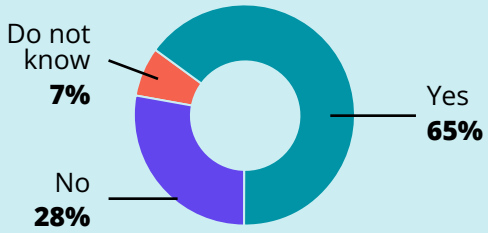
In organizations with threat assessment teams, only 11 percent of security professionals said an after-action report of an incident showed such missed signs.

The research also probed what effect the COVID-19 pandemic had on how organizations approach active assailant preparedness. Keeping in mind this was a broad-based survey directed primarily at ASIS members and customers, participants came from various sectors, including manufacturing and healthcare, two sectors where post-pandemic work patterns likely reflect substantially the same patterns as before the pandemic, as well as financial services and government agencies, which may have undergone significant transitions.

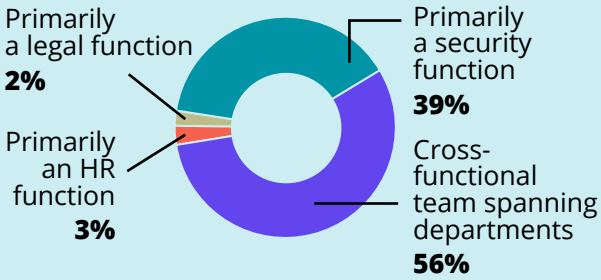
Almost half of respondents said there were more remote workers or hybrid workers than before than pandemic. A factor that impacts effective incident response: 17 percent said it was harder to know who is in a facility or on a campus at any given time. Interestingly, 8 percent said they reduced frontline security staff while 12 percent said they increased it, and 28 percent of security professionals said their physical security priorities had changed significantly. Here is the full list of factors the survey asked about:

Figure 3.4: Threat Assessment Teams

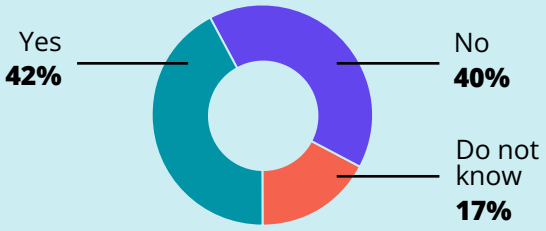
Does Your Organization Have a Threat Assessment Team That Evaluates Potential Active Assailant Threats?



How Is the Threat Assessment Team Managed?



In Past 12 Months Did Threat Assessment Team Take Action That Prevented Serious Incident?



Percent of Security Professionals Agreeing With These Statements	
We have substantially more remote employees or students	35%
We implemented a hybrid work schedule	48%
There has been little to no change where people work	29%
Knowing who is in our facility or on campus is more difficult	17%
We decreased the number of front-line security FTEs	8%
We increased the number of front-line security FTEs	12%
We increased reliance on video surveillance	25%
Our physical security priorities changed significantly	28%

Despite the change, a majority of security professionals (55 percent) said their organization's approach to active assailant preparedness did not change significantly since before the pandemic. Approximately one-quarter said the pandemic introduced new variables making active assailant preparedness more complex, and a quarter said an increase in violence made preparedness even more important. Eight percent said their organizations placed less emphasis on active assailant preparedness.

HOW PREPARED ARE ORGANIZATIONS FOR AN ACTIVE ASSAILANT INCIDENT?

The survey asked security professionals to rank how effective they think their organization would be across three dimensions:

- How confident are you that your organization could provide a detailed situational awareness report by the time first responders arrive in the event of an active assailant?
- How confident are you that your staff knows what to do in the event of an active assailant incident?
- How confident are you that your organization is prepared for an active assailant incident?

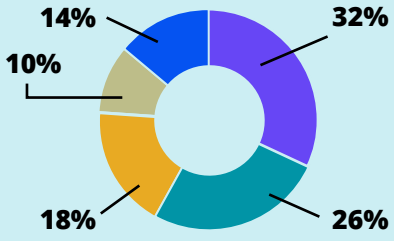
Given a five point scale, a 1 was labelled "not at all confident," a 2 was "somewhat confident," a 3 was "medium level of confidence," a 4 was "mostly confident," and finally a 5 was "highly confident."

In general, given the magnitude of what it means for an active assailant situation to spiral out of control, a response of "mostly confident" or better is a desired benchmark, and by that benchmark, most organizations fell short (see Figure 4.1).

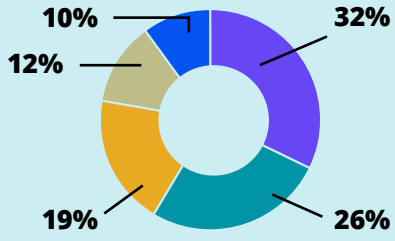
Overall, 46 percent of security professionals were mostly or highly confident they could provide a detailed situational awareness report by the time first responders arrive during an active assailant incident. Of the three questions, security professionals were most confident about this one, but still, the number falls short of what is desired. Petrino pointed out that low scores on the other ones are understandable—it's realistic to think that the utter chaos of an active shooter would throttle the confidence of anybody responsible for preparing for it. But this is the one security professionals should be getting right.

Figure 4.1: Active Assailant Training

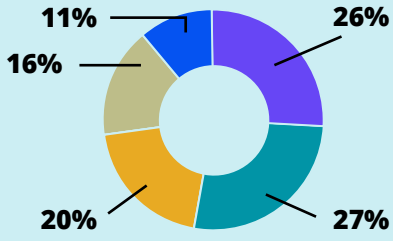
How Confident Are You That You Could Provide a Detailed Situational Awareness Report to First Responders During Active Assailant Incident?



How Confident Are You That Your Staff Knows What to Do in the Event of an Active Assailant Incident?



How Confident Are You That Your Organization Is Prepared for an Active Assailant Incident?



Highly confident
Mostly confident
Medium confidence
Somewhat confident
Not at all confident

"For any midsize organization—a hospital, a school, whoever—if they don't already have a relationship with local law enforcement, then they're already almost too late," he said.

On the ultimate question—is their organization prepared for an active assailant incident—only 37 percent are mostly or highly confident, and 16 percent are not at all confident. While not exactly inspiring, it does mark an improvement over prior years. The 2023 and 2020 surveys asked the question slightly differently, asking security professionals how prepared their organizations were for an active shooter event, with the range being not at all prepared to very much prepared. Adding those who responded very much prepared and quite a bit prepared together as a comparison, 29 percent felt prepared in 2023, and 34 percent felt prepared in 2020.

FACTORS THAT IMPROVE ACTIVE ASSAILANT PREPAREDNESS

Everyone in security knows it is incredibly hard to measure security's effectiveness and impact. How do you measure the absence of something happening? Potentially a little more measurable: How do you assess whether or not a devastating active assailant incident was less devastating because you had prepared for it?

The times when there is an identified threat that is mitigated with little or no adverse consequences are success stories that underscore the importance of security measures. However, these incidents are not conducive to measuring via a broad-based survey. For this style of research, we rely on looking at what factors make a difference in the confidence levels as detailed in the previous section. In research of other security issues, security actions that led to increases in confidence of 15 to 20 percent indicated the recommended practices organizations could undertake to improve their security posture.

That's why the findings from this survey were remarkable. Anyone who has read the report up to this point will not be surprised at the factors cited in this section. Indeed, most security professionals could tell you these factors would make a difference without any research. However, the strength of the correlations are powerful.

To get the correlations, researchers cross-tabulated questions that focused on each of the factors with the three confidence questions presented in the previous section. The number-crunching is significant, but this report presents the findings across four factors to show just how consistent and strong the findings were. Security professionals should focus on these four areas if they want to improve their active assailant preparedness:

- Generating and following a plan
- Communications measures
- Training
- Threat assessment teams

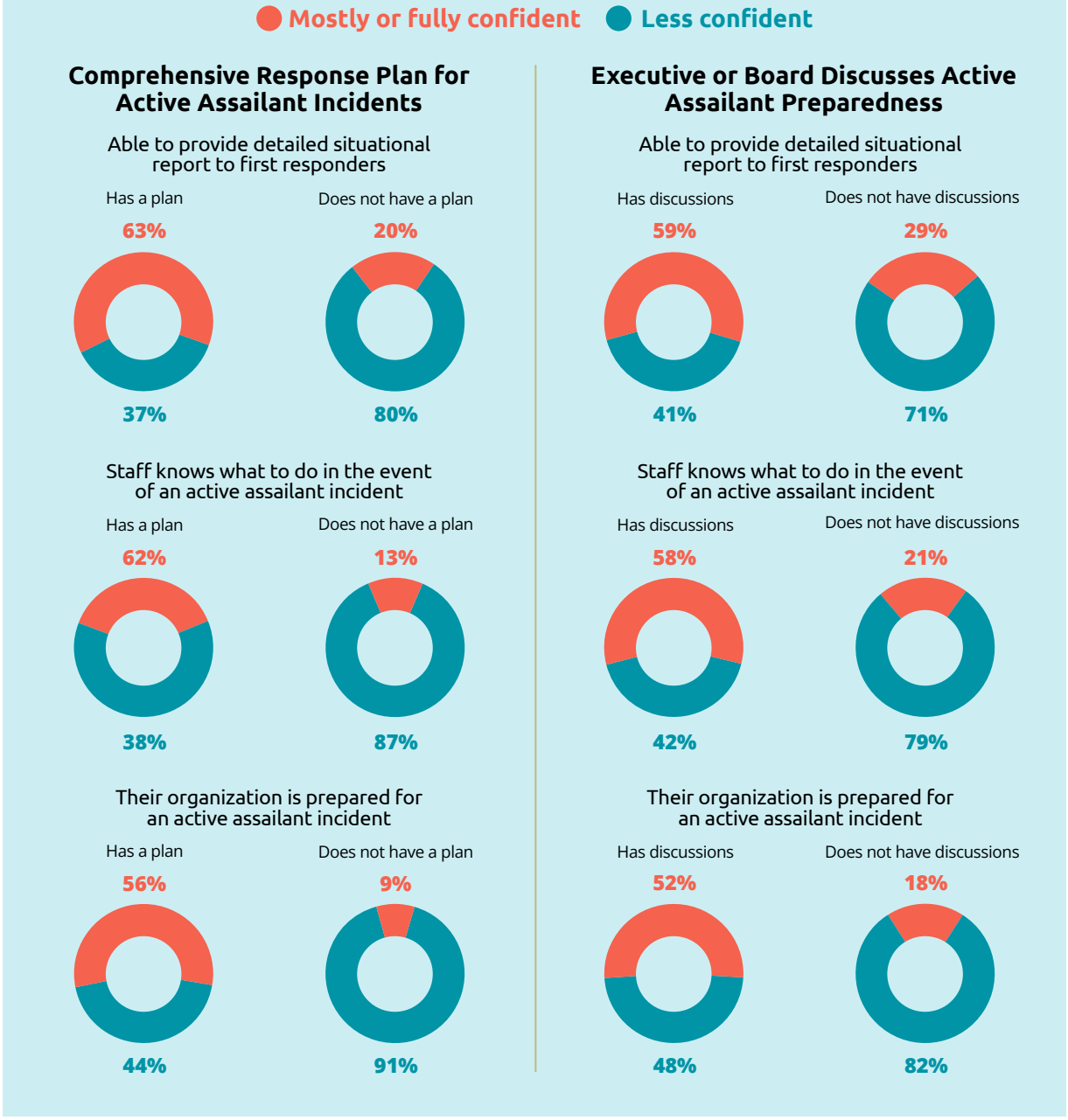
GENERATING AND FOLLOWING A PLAN

The survey asked the question directly: Does your organization have a comprehensive response plan in place for active assailant incidents? Of the 61 percent who have such a plan, 56 percent are either highly or mostly confident that their organization is prepared for an active assailant event. Those without a plan? Only 9 percent said they were highly or mostly confident (see Figure 5.1).

Similarly, another indicator of planning for active assailants is a question that asked if an organization's board or executive team discussed active assailant preparedness. Fifty-eight percent reported that it was, while 24 percent said it was not and 19 percent did not know. Security professionals at organizations that have executive- or board-level discussions are much more confident in their organization's preparation for an active assailant: 52 percent are highly or mostly confident, which compares to 18 percent of security professionals at organizations where the board conversations do not take place.

The percentages change, but the strong correlation between these two questions persists through the other two confidence questions, which cover the ability to provide a detailed situational awareness report and staff knowing what to do during an incident. The complete breakdown of how these factors impacted confidence levels follows.

Figure 5.1: Effect Planning Has on Confidence of Active Assailant Preparedness



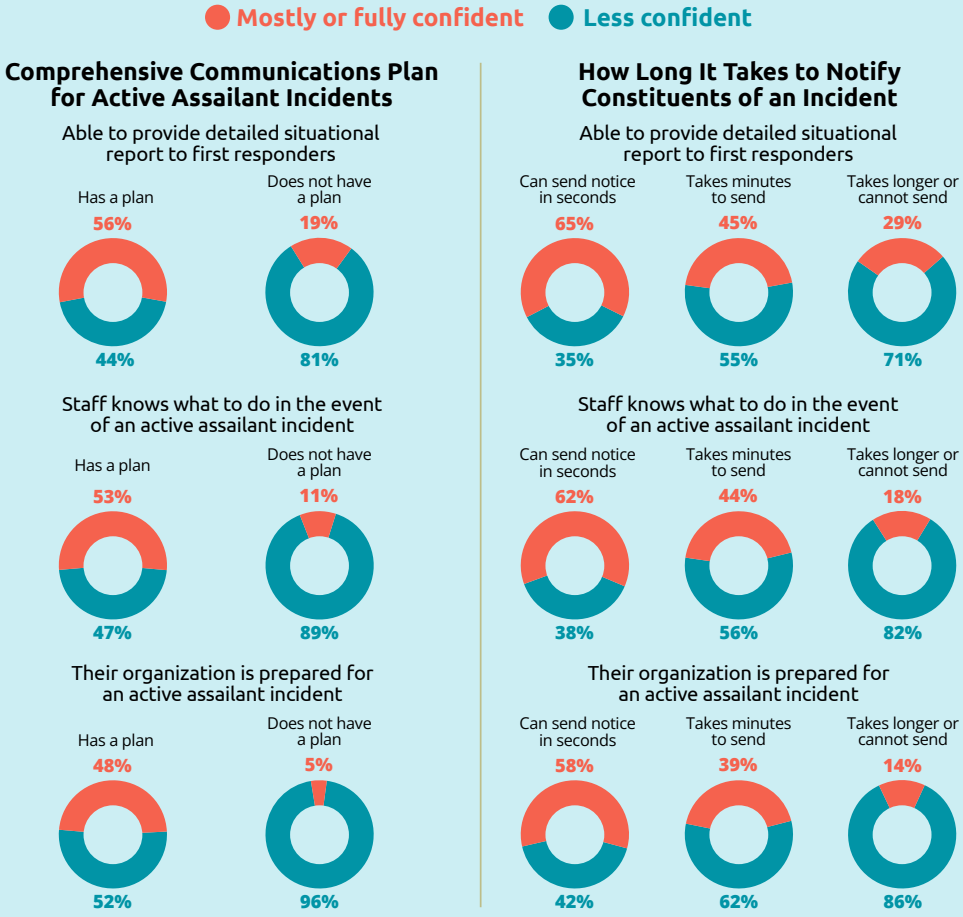
COMMUNICATIONS PLANNING AND NOTIFICATION TECHNOLOGY BOOST CONFIDENCE

Just as with having an overall plan, having a specific communications plan in place for active assailant incident is a big boost of confidence for security professionals. For those with communications plans, 48 percent are highly or mostly confident their organization is prepared for an active assailant incident. That drops to just 5 percent for those without communications plans.

The disparity is not quite as stark when looking at the length of time it would take to get a notification to employees, students, or other constituents, but it is still a very strong correlation that gets stronger the quicker the communication can happen. A majority of security professionals at organizations with the capability to get a notification out in mere seconds are highly or mostly confident their organization is prepared for an active assailant incident (58 percent) compared to 39 percent of security professionals at organizations that take minutes to get a notification out and just 14 percent for those who take longer or do not have the capability.

The full breakdown of the confidence data compared to communications related follows.

Figure 5.2: Effect Communications Has on Confidence of Active Assailant Preparedness



ACTIVE ASSAILANT TRAINING COMPARISON

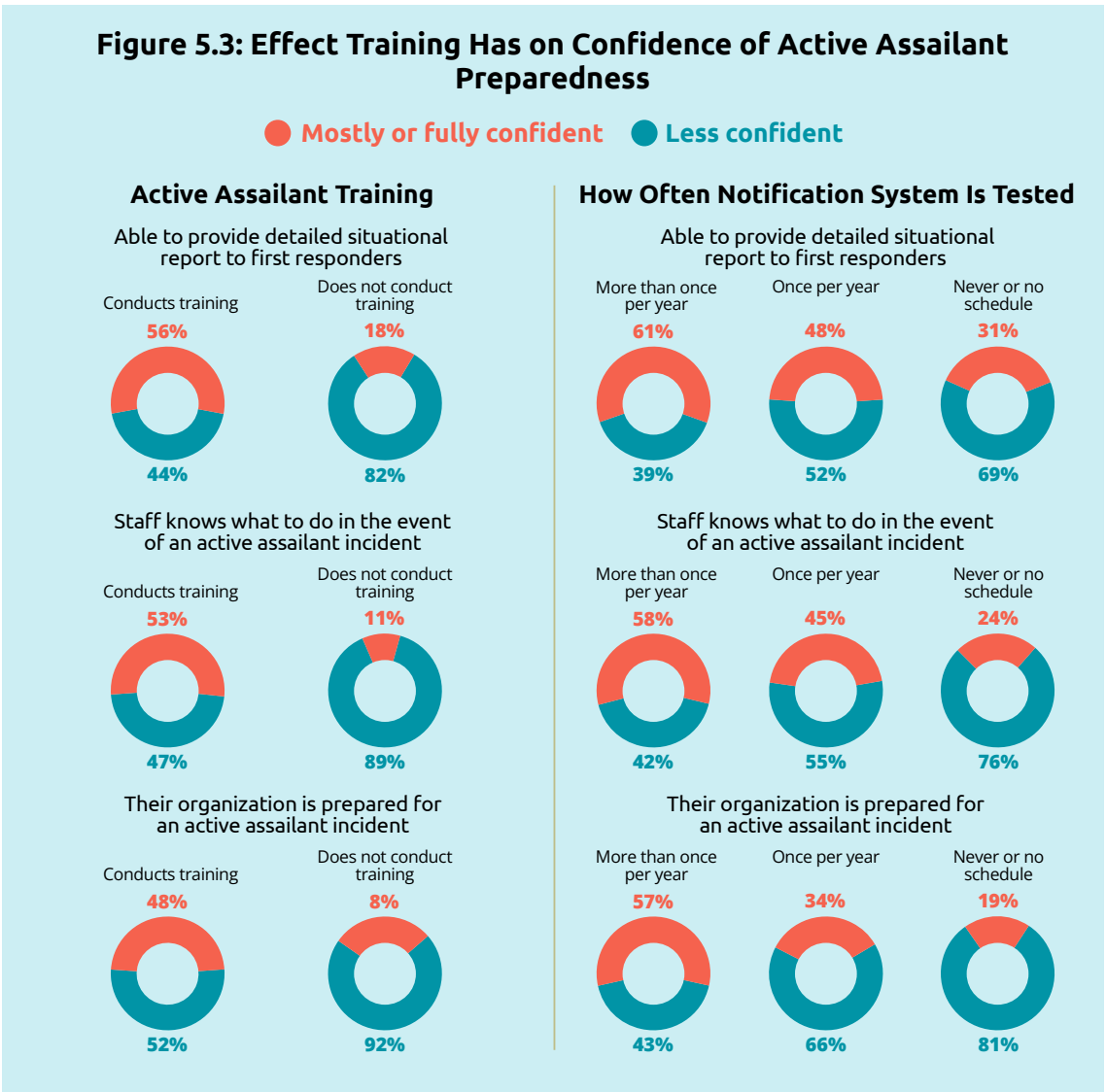
Similar to having a plan, it stands to reason that if you train or test your readiness, you will be more confident in your ability to deal with a situation than if you do not train or test for it. The point is the same: it's the difference in confidence level that is so impressive and really underscores the need for organizations to take these actions.

When it comes to training, the difference in confidence between those with specific active assailant training in place and those that do not train is 40 percent (48 percent of those with training are highly or mostly confident; 8 percent of those without training are highly or mostly confident).

The survey also asked how often organizations tested their system for sending alerts to employees. Again, the differences are not quite as stark, but they are still significant, and the more often you test, the more confident you are.

The full breakdown of the confidence data compared to training and testing follows.

Figure 5.3: Effect Training Has on Confidence of Active Assailant Preparedness



THREAT ASSESSMENT TEAMS AND PREPAREDNESS

Threat assessment teams are primarily a preventative function when it comes to workplace violence and active assailants. Underscoring the notion that prevention is incredibly important to being prepared for active assailants, deploying the teams correlates strongly with security professional confidence. Just over half (51 percent) of security professionals at organizations that use threat assessment teams are highly or mostly confident their organizations are prepared for an active assailant incident, compared to just 13 percent at organizations that do not use threat assessment teams.

The full breakdown of the confidence data compared to threat assessment teams follows.

Figure 5.4: Effect Threat Assessment Teams Have on Confidence of Active Assailant Preparedness

RESEARCH METHODOLOGY

The 2024 ASIS-Everbridge Active Assailant Preparedness survey was deployed in June and July 2024 using SurveyMonkey. It was promoted to ASIS International members and customers via email, newsletters, and social channels, and to Everbridge contacts. A total of 701 people participated in the survey and 540 people completed it. All answers were counted in the results whether or not they completed the survey. This results in a margin of error of plus or minus 4 percent at a 95 percent confidence interval. Not every participant was asked every question, so the margin of error on some questions may be higher.

The 2023 and 2020 surveys were conducted similarly. With 653 and 477 completed surveys in each of those years respectively, they also have a margin of error of plus or minus 4 percent.

There is likely to be some bias introduced into the data because of how it was promoted. Participants knew they were answering a survey on active assailant preparedness, showing they likely had an interest in the subject. That coupled with the fact that participants were overwhelmingly ASIS members or customers, it is likely they have a higher knowledge level about active assailant preparedness issues than people who are not ASIS members or customers.

The survey asked several demographic questions, and the results were similar to other security topic research projects that ASIS has completed in the last year. In addition, the 2024, 2023, and 2020 active assailant surveys all had demographic similar demographic results.

As is typical for ASIS research, there were many respondents from large companies—22 percent had more than 10,000 employees—though just under half (47 percent) had 1,000 or fewer employees (with the rest, approximately one-third, falling in between). Most respondents, 43 percent, were with organizations that had multiple locations or campuses in multiple regions. Thirty-four percent had multiple locations in a single region, and 19 percent had a single location (4 percent wrote in an alternative geographic footprint answer).

Nearly 2 in 3 (65 percent) of respondents were from North America, which is slightly higher than normal for ASIS surveys, perhaps suggesting that the topic was more germane to North America than other regions. Africa; Asia; South America, Central America, and the Caribbean; and Europe were the next highest regions, but all were within 5 percent of each other. The exact order changes from survey to survey, but these regions are usually similar to each other in participation.

The survey also tends to reach higher-level security professionals most. Overall, one quarter of respondents (26 percent) were chief security officers, vice presidents of security, or directors of security. Another 30 percent were senior managers or managers of security, and five percent were frontline security. Seven percent said they were security consultants or business partners, and the rest had a variety of titles and roles.

Survey participants came from a variety of sectors with no one sector dominating the research. The single largest sector was manufacturing, which only reached 7 percent. The rest were spread across 38 other sectors or wrote in a different choice.