# The Executive Threat Environment

Benchmarking Research on Risk-Based Approaches to Executive Protection

ASIS INTERNATIONAL | SECURITY ISSUES RESEARCH

Sponsored by

everbridge™

## Contents

ASIS INTERNATIONAL
*Advancing Security Worldwide®*

ASIS International thanks Everbridge for their sponsorship of this research. www.everbridge.com

everbridge™

## Introduction and Key Points

On 4 December 2024, a man upset with the U.S. healthcare system and insurance company United Health in particular shot and killed United Health CEO Brian Thompson on a street in New York City. Organizations have a duty of care to protect all employees, and, as the United Health assassination showed, the protection of top executives has always presented a unique set of challenges for security professionals.

Together with partner Everbridge, ASIS International Security Issues Research undertook a study to capture the current status and practice of executive protection. 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 corporate executive protection.

Approximately 400 people completed the security professionals survey and 110 completed the consultants survey, providing a trove of a data presented in this report.  Here are some of the key findings.

The study validates what anecdotally is obvious: organizations have increased the attention paid to executive protection: 42 percent report there is significantly more emphasis when compared to 18 months ago. (See page 7 for more.)

High-profile incidents are only one factor driving the increased attention, security professionals report growing numbers of public threats as well as direct threats to executives. (See page 7 for more.)

One area for improvement: The top challenges security professionals have implementing EP measures involve a lack of value placed on EP by executives themselves. At the same time, security professionals report that their programs are deficient in areas that could be used to show that very value, things like setting key performance indicators (KPIs) and data collection to show the ROI of EP. (See pages 8 and 10 for more.)

Other possible areas for improvement are areas that security professionals say are highly important but report that they either do not have the capability or only partially have the capability. Included in this category is the capability to protect digital assets, behavioral threat profiling and anomaly detection, and monitoring online threats or expressions of anger at specific locations, organizations, or executives. (See page 9 for more.)

At a quarter of organizations, security has little or no role in making executive travel arrangements. (See page 13 for more.)

Intelligence monitoring—necessary for quick identification of emerging threats—would seem to be a necessity for any travel EP program, but 30 percent of security professionals report their organizations only deploy intelligence monitoring with regard to traveling executives when a threat assessment says it is needed—and another 13 percent report they rarely or never engage in intelligence monitoring regarding executive travel. (See page 13 for more.)

45 percent of organizations provide close protection all or most of the time when an executive is on travel. Another 24 percent do so when threat assessments say it is needed, and 21 percent rarely or never provide close protection when an executive is traveling.(See page 13 for more.)

One-quarter of organizations rarely or never conduct travel safety briefings with executives. Those that do focus on the executive but omit briefings for family or staff traveling with the executive, or GSOC staff, who often are the first to access intelligence that may be important. (See page 15 for more.)

25 percent of organizations have never conducted scenario training or tabletop exercises based on possible executive protection incidents. (See page 16 for more.)

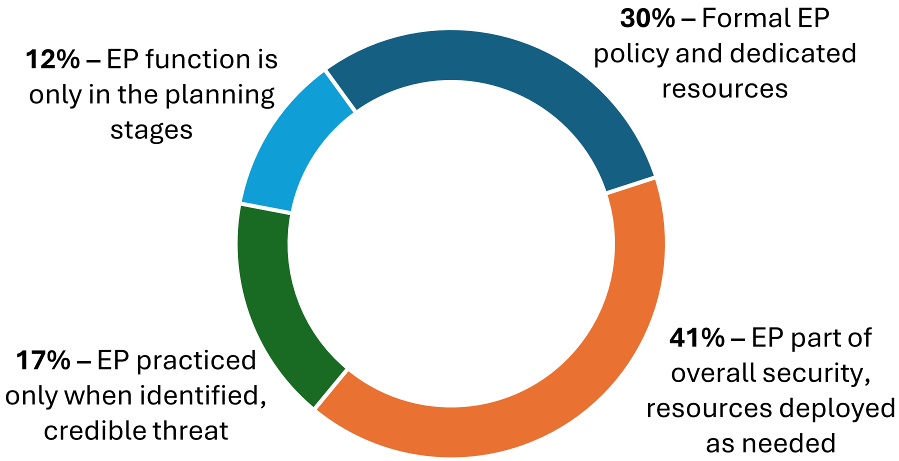
## Approach to Executive Protection

The survey asked security professionals where their executive protection program fell on a continuum of having a formalized and dedicated EP function to practicing EP only when there is a threat making it necessary to not practicing EP at all.*

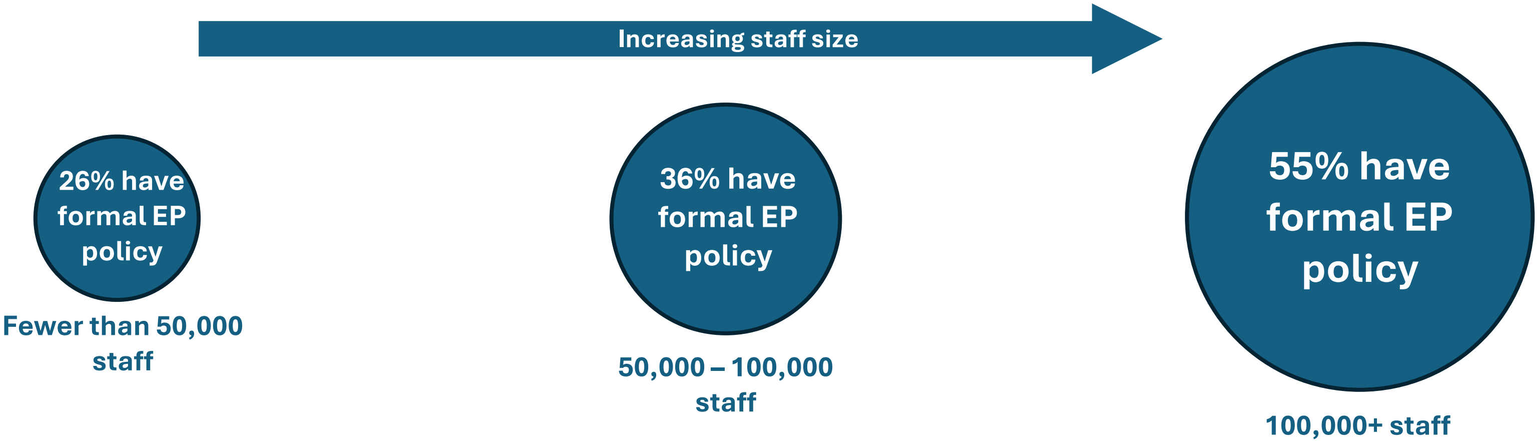
Overall, organizations tended to either have a formalized EP policy with dedicated resources (30 percent) or practice EP as part of a larger security policy with resources deployed as needed. Fewer organizations put resources into EP only when there were identified, credible threats (17 percent).

The very largest organizations in the survey, those with more than 100,000 employees or students, were far more likely than other organizations to have a formal EP program, at 55 percent. Organizations with 50,000 to 100,000 employees or students, at 36 percent, were also more likely than smaller organizations to have the most formal EP program.

## Formality of EP Function



## Larger Organizations Are Much More Likely to Have a Formal Executive Protection Policy



Increasing staff size

26% have formal EP policy

Fewer than 50,000 staff

36% have formal EP policy

50,000 – 100,000 staff

55% have formal EP policy

100,000+ staff

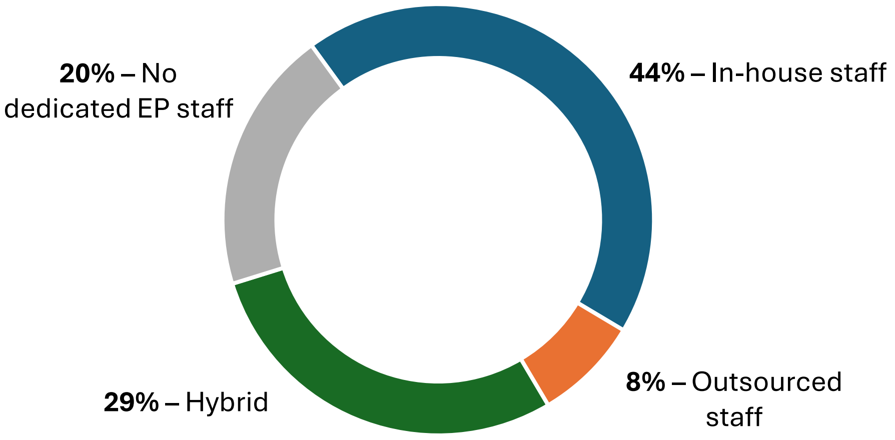
* 7 percent of the survey participants reported that they rarely or never deployed EP and had no plans to do so. These people are excluded from these results and did not take the rest of the survey. Also note: The research was promoted as executive protection research, which likely resulted in self-selection bias. The actual number of organizations not practicing EP is likely higher.

## How Organizations Approach Executive Protection Staffing

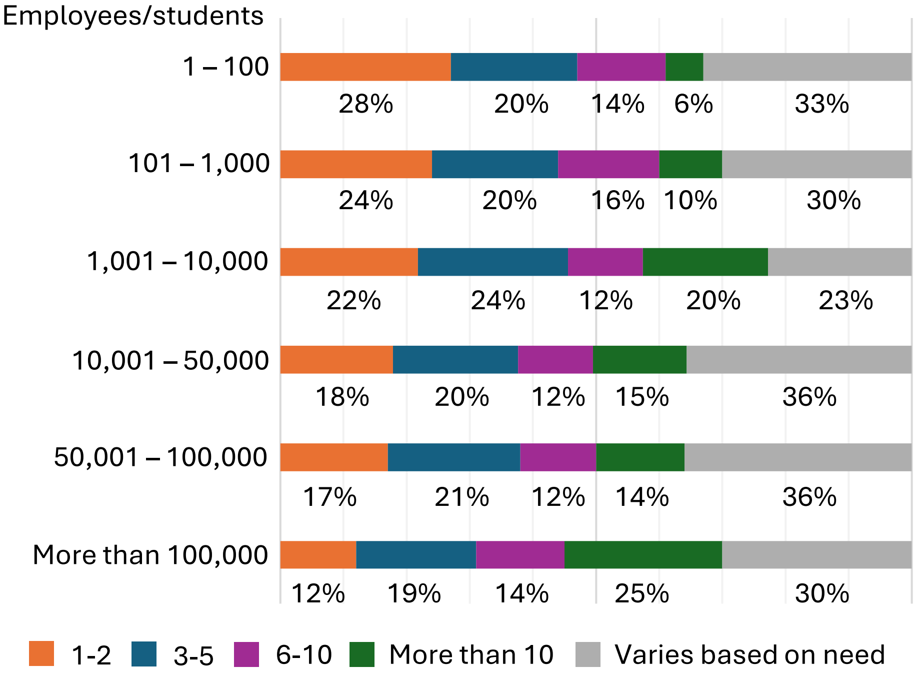
Excluding respondents who reported they were only in the planning stages of an executive protection program, 80 percent report that they dedicate human resources to the function. Nearly half (44 percent) report their EP staff are part of the organization's security staff, 8 percent report that they primarily use outsourced EP staff, and 29 percent report a hybrid of in-house and outsourced staff.

Just like larger organizations were more likely than smaller organizations to have a formal EP function, they are also more likely to have dedicated human resources to the function and to protect more execcutives.

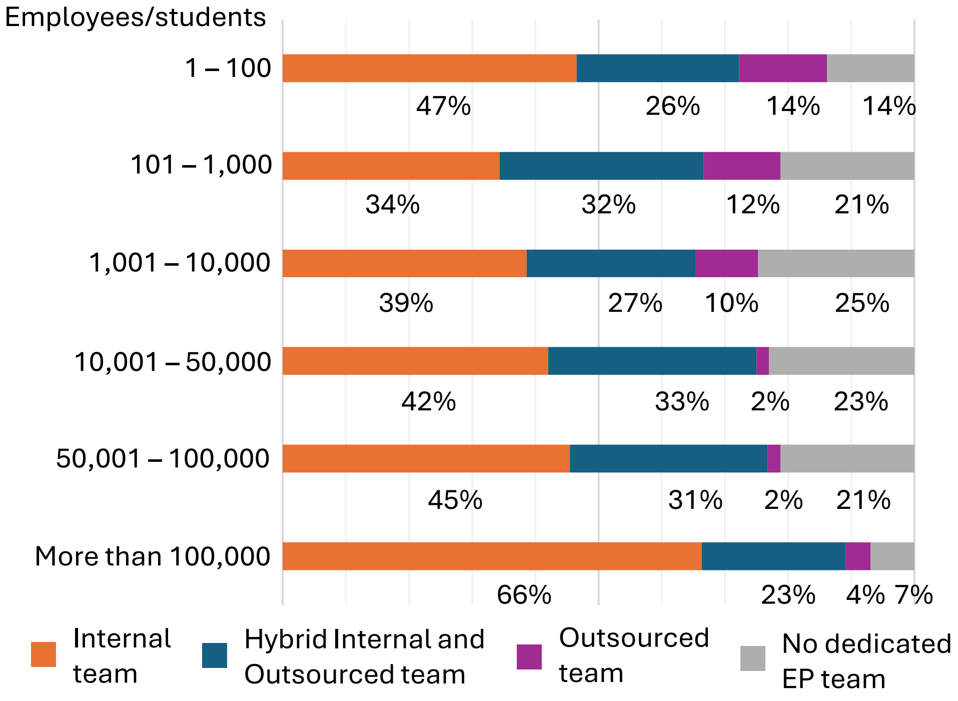
## Executive Protection Staffing



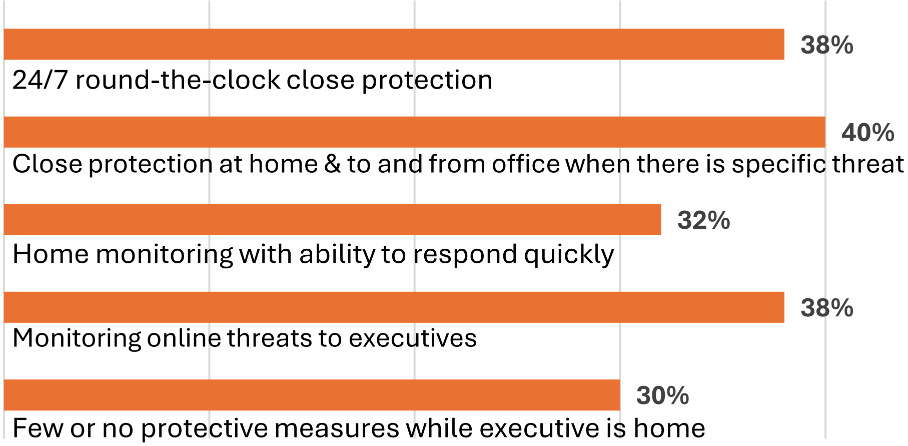
## Number of Executives Protected by Organization Size



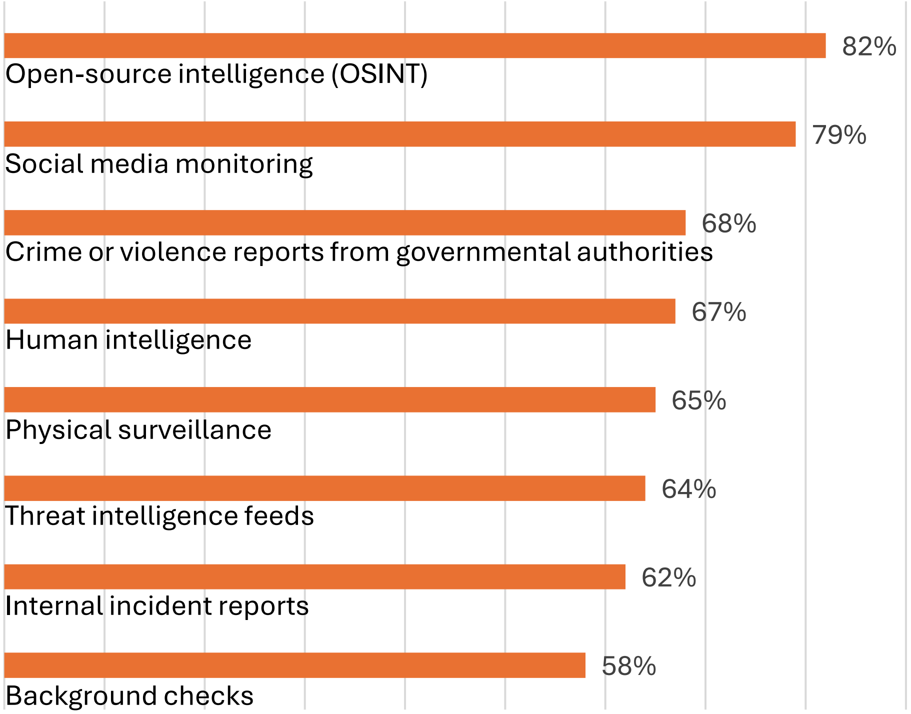
## EP Staffing by Organization Size



## Day-to-Day Level of Executive Protection



## Methods Used to Find/Assess EP Threats

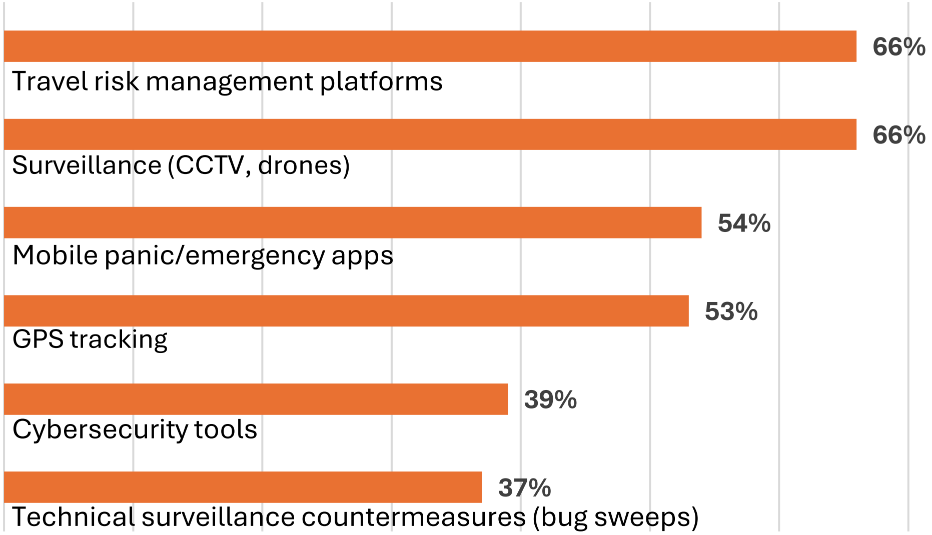


## Executive Protection Management Practices

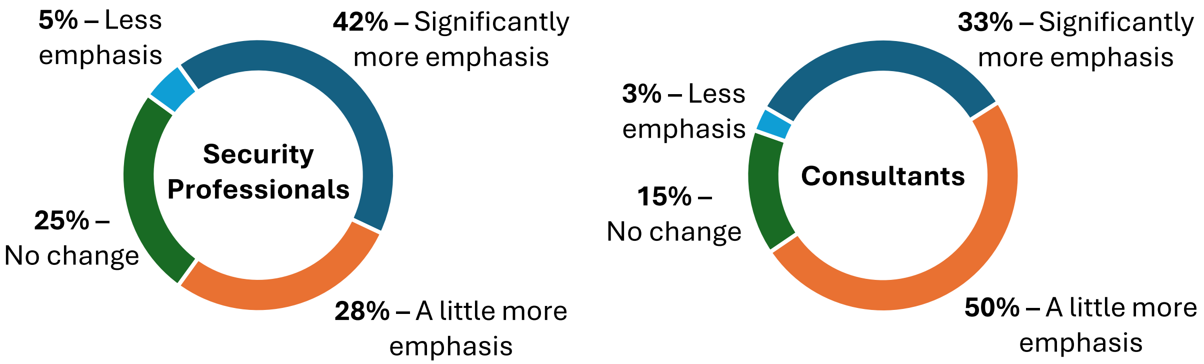
The results on this page reflect only those organizations that reported they have an EP function in place. Examining day-to-day EP practices, nearly one-third (30 percent) of organizations do not provide significant services to executives while they are in their homes. From none to the most, 38 percent of security professionals say the most protected individual at their organization receives 24/7 close protection, while 40 percent report they provide close protection at home and to and from the office when there is a specific threat. In addition, one-third (32 percent) say they monitor executives' homes and can respond quickly if needed.

Security professionals use a variety of methods to find and assess threats to executives, with OSINT leading the way. Every method asked about in the survey scored higher than 50 percent use. The most prevalent technologies used in EP are travel risk management platforms, surveillance, mobile or emergency apps, and GPS tracking. Less than half of organizations use specialized cybersecurity tools or bug sweeping technology.

## Technologies Used in Executive Protection

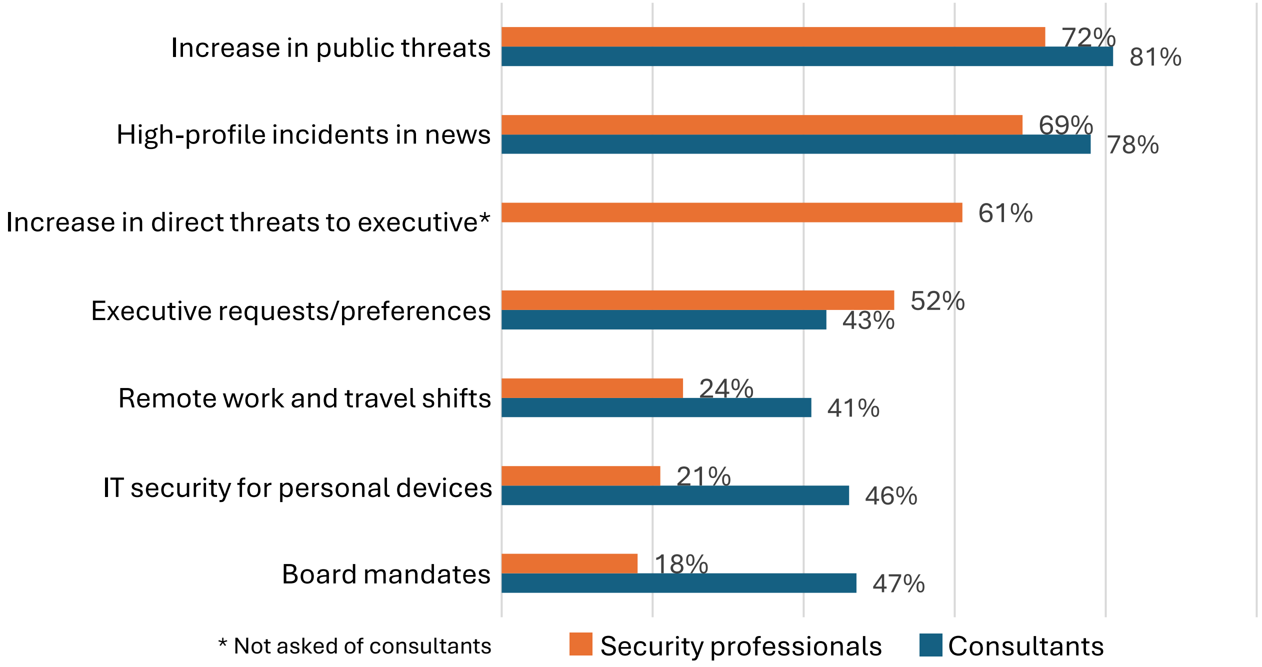


## Are Organizations Placing More Emphasis on Executive Protection?



(Compared to 2 years ago)

## Reasons for Increased EP Emphasis



* Not asked of consultants

## Executive Protection Is Getting More Attention

More than two-thirds of security professionals report that executive protection is getting more attention now than it was two years ago, with 4 in 10 saying EP was now getting "significantly more emphasis."

The murder of United Health's Thompson no doubt contributed to this emphasis. Asked to select reasons for the increased emphasis, 69 percent of security professionals selected "high-profile incidents in the news," which was the second-most cited reason. "Increase in public threats" led the way with 72 percent. Far fewer reported that remote work or shifting travel demands (24 percent) or board mandates (18 percent) were reasons for increased emphasis.

Consultants, too, see more emphasis on executive protection, though the change is more muted, with 50 percent saying "there is a little more emphasis." Consultants also chose "increase in public threats" (81 percent) and "high-profile incidents in the news" (78 percent) as the most likely reasons for increased emphasis. However, consultants selected board mandates and shifts in remote work and travel about the same amount as the other choices: IT security for personal devices and executive requests.

## The Problem with Executive Protection Is the Executives

The top two executive protection challenges security professionals identified are budget constraints, cited by 58 percent, and executive noncompliance, 47 percent.

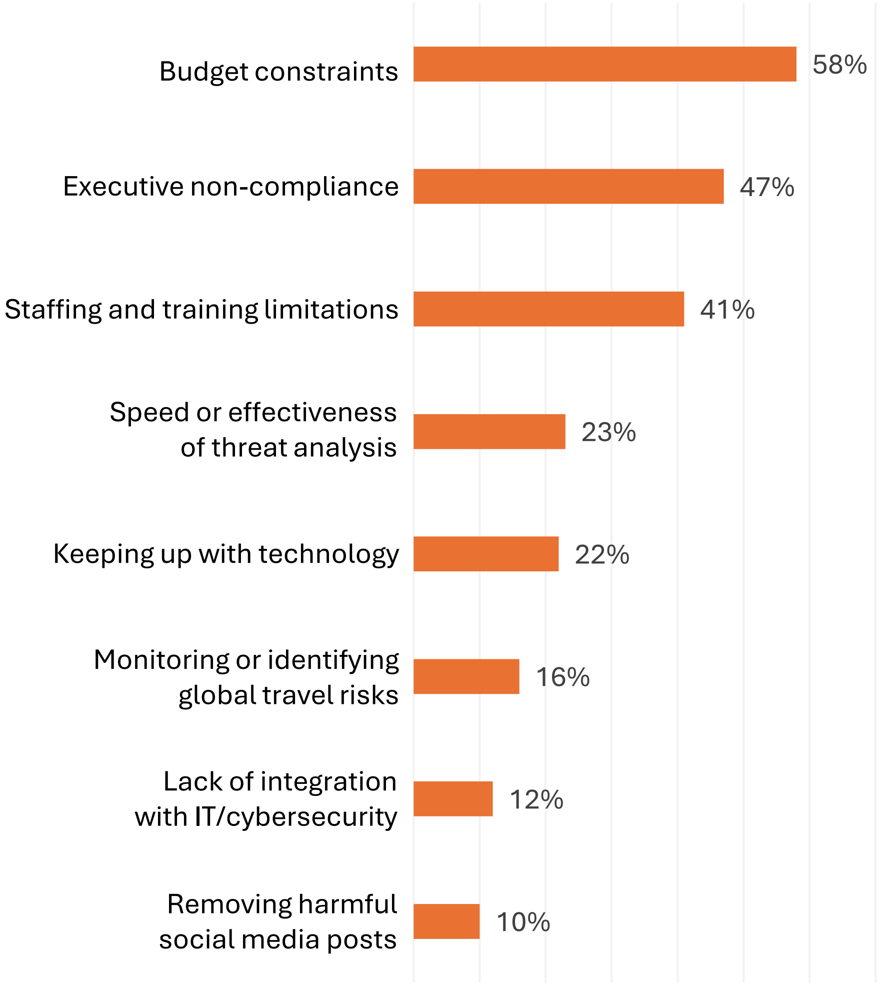
These two challenges are related in that both signify that an organization's top executives do not see the value in executive protection.

The consultant's survey asked an open-ended question: "What is your best advice for corporate security leaders who face executives who resist certain executive protection processes or methods?" One answer in particular encapsulates most of the of the advice. Here it is (slightly edited for clarity):

"My best advice is to align protection strategies with the executive's business goals and personal priorities. Avoid using fear-based messaging. Instead, communicate the value of protection in terms of business continuity, reputation management, and operational efficiency. Build trust by being discreet, professional, and solution-oriented. Involve them in decision-making processes, offer options rather than ultimatums, and always back your recommendations with clear, real-world examples and risk intelligence. Ultimately, the key is to position security as an enabler—not an obstacle—of their success."

The only other challenge that had traction in the survey was staffing and training limitations, which was cited by 41 percent of security professionals. See page 16 for benchmarks on the kinds of trainings organizations provide for both EP personnel and protectees.

## Challenges to Effective EP



## Capabilities Where Importance Outpaces Adoption

| Capability | Highly important | Fully have capability | Difference |
|---|---|---|---|
| Protection of digital assets/secure communications | 57% | 42% | 15% |
| Behavioral threat profiling and anomaly detection | 48% | 33% | 15% |
| Monitoring online threats or expressions of anger at specific location, organization, or executive | 65% | 51% | 14% |
| Predictive risk analytics (risk escalation forecasts) | 52% | 39% | 13% |
| Real-time open-source intelligence (OSINT), social media monitoring, and digital threat detection | 63% | 50% | 13% |
| Automated situational reports and threat, vulnerability, and risk (TVR) report generation | 42% | 30% | 12% |
| Automated after-action reports, data repository, and analytics | 36% | 26% | 10% |

## Areas to Reassess EP Resource Allocations: Capabilities vs. Importance

The survey presented 22 different capabilities and asked security professionals to rate each on the extent to which they had the capability and the importance of the capability to the EP program.

The capabilities were divided into two sets, one set of 12 examines technical or physical capabilities. The other set of 10 examines specific EP practices—many of which are related to the technical capabilities. Pages 11-12 present the full dataset for benchmarking purposes. This page looks at the capabilities where more security professionals said the capability was highly important than said they fully have the capability. For the seven capabilities listed in the table at left , at least 10 percent more security professionals said the capability was highly important than reported their organizations were fully functional in that capability.

For example, the most important technical capability—"real-time open-source intelligence, social media monitoring," which was rated as highly important by 63 percent—is related to the most important practice—"monitoring online threats or expressions of anger at specific location, organization, or executive," which was rated as highly important by 65 percent. While roughly half of security professionals report being fully capable in these areas, that leaves half of organizations that are only partially capable or have no capability.

Other areas to consider:

- Protection of digital assets/secure communications
- Behavioral threat profiling and anomaly detection
- Predictive risk analytics
- Automated situational reports and threat, vulnerability, and risk report generation
- Automated after-action reports, data repository, and analytics

## Areas to Reassess EP Resource Allocations: Executive Support

Other possible areas of opportunity are derived from the capabilities on both lists that were rated lowly in both adoption and importance. Page 8 described how the most prevalent EP challenges are ones that deal with the value top executives place on EP. It's notable that two capabilities—"automated after-action reports, data repository, and analytics" and "data logging and exportable analytics for EP ROI calculation"—were not deemed important by security professionals and were not in place in most organizations.

However, both capabilities fall into areas that could help security professionals build the case of EP value.

Underscoring the opportunity, the bar chart below shows the results from a survey question about how organizations measure the effectiveness of their EP programs. It's such a business truism that it's cliché: What gets measured gets attention. It says a lot that more than a third of security professionals report that there is no formal evaluation process for EP and less then half record basic data, such as incident tracking, or identify and measure KPIs.

## Capabilities Organizations Do Not Have

**(Percentage of those with only partial or no capability in the area.)**

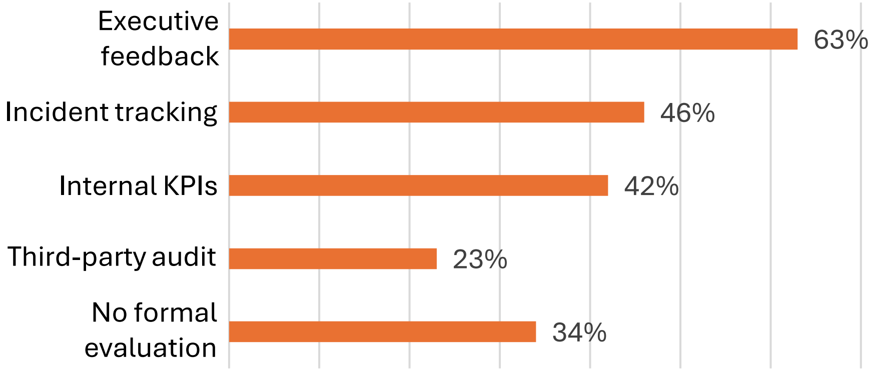
| | |
|---|---|
| Automated situational reports and threat, vulnerability, and risk (TVR) report generation | 69% |
| Close protection agents working with family (immediate and extended) of the executive | 71% |
| Customizable dashboard and team permission levels | 72% |
| **Automated after-action reports, data repository, and analytics** | **73%** |
| **Data logging and exportable analytics for EP ROI calculation** | **78%** |

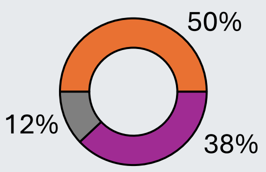
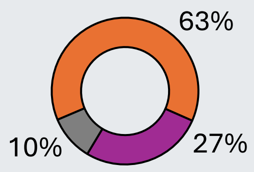
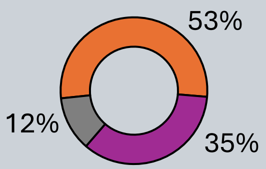
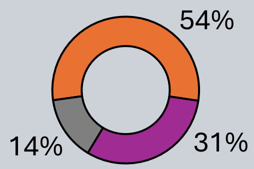
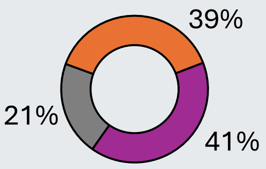
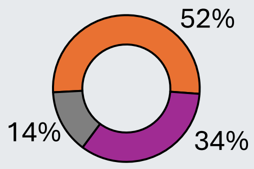
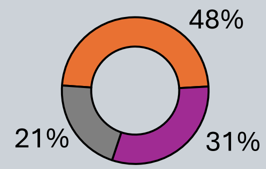
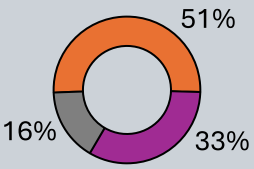
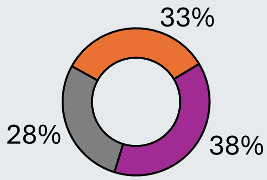
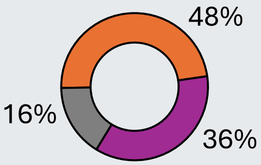
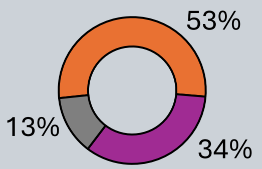
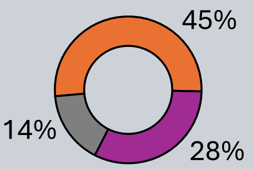
## Least Important Capabilities

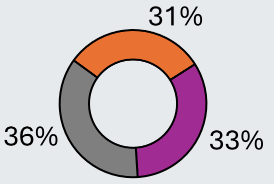
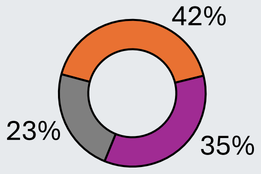
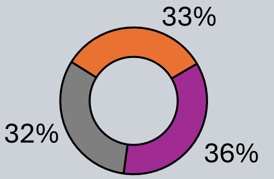
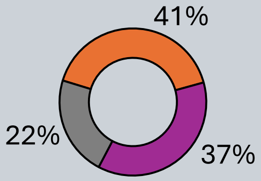
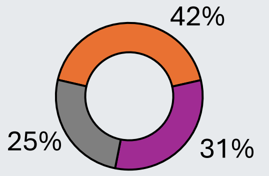
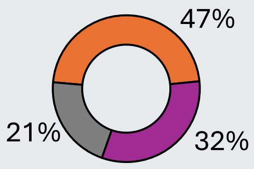
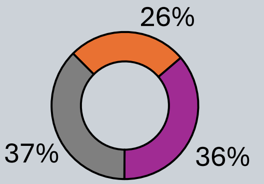
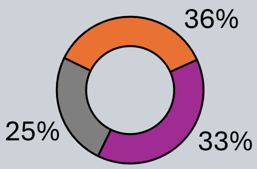
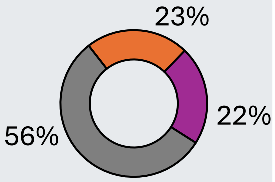
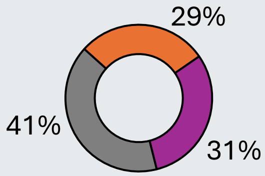
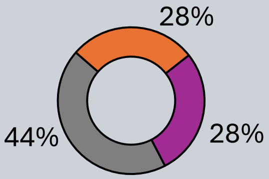
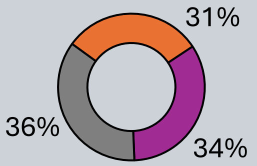
**(Percentage who rated capability as low importance.)**

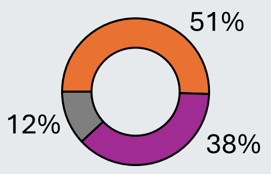
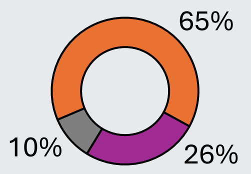
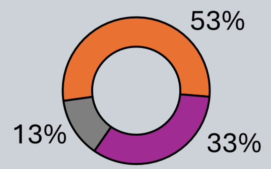
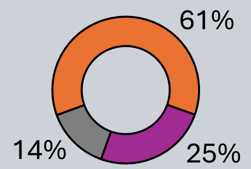
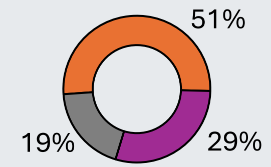
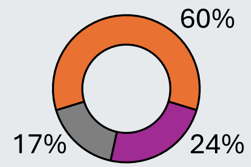
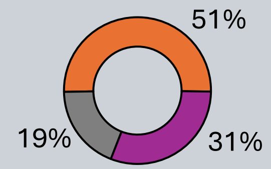
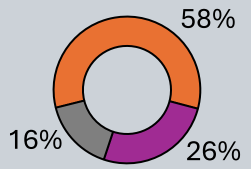
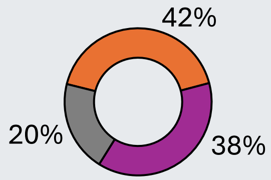
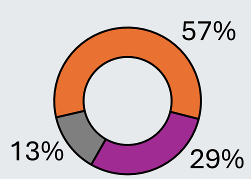
| | |
|---|---|
| **Automated after-action reports, data repository, and analytics** | **25%** |
| Close protection agents working with the executive on a daily basis | 26% |
| Customizable dashboard and team permission levels | 36% |
| **Data logging and exportable analytics for EP ROI calculation** | **41%** |
| Close protection agents working with family (immediate and extended) of the executive | 46% |

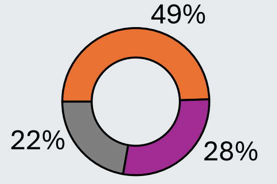
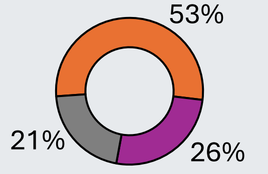
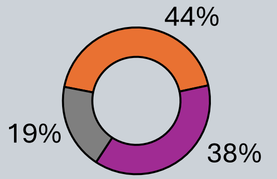
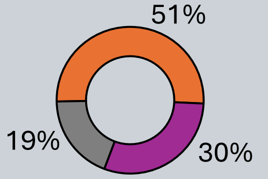
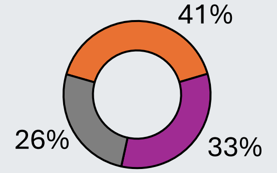
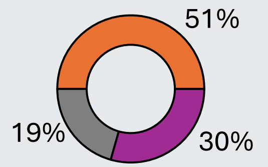
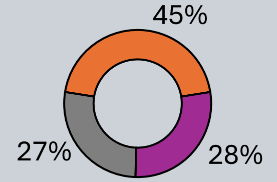
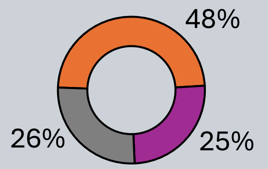
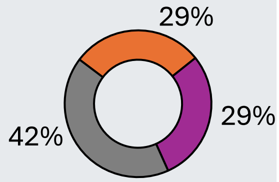
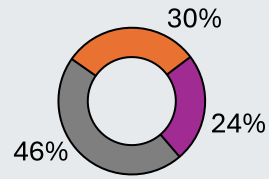
## How Is the Effectiveness of Your Executive Protection Program Evaluated?



| Technical Capability | Have capability | Importance |
|---|---|---|
| Key | ● Fully ● Partially<br>● Not at all | ● High ● Medium<br>● Low |
| Real-time open-source intelligence, social media monitoring, and digital threat detection |  |  |
| Security training and briefings customized per user |  |  |
| Predictive risk analytics (risk escalation forecasts) |  |  |
| Multi-channel alert system (SMS, app, email, voip integration) |  |  |
| Behavioral threat profiling and anomaly detection |  |  |
| Travel authorization, risk, and itinerary monitoring |  |  |

| Technical Capability | Have capability | Importance |
|---|---|---|
| Key | ● Fully ● Partially<br>● Not at all | ● High ● Medium<br>● Low |
| Automated situational reports and threat, vulnerability, and risk (TVR) report generation |  |  |
| Digital footprint monitoring and sentiment analysis |  |  |
| Location-based geofencing alerts and tracking |  |  |
| Automated after-action reports, data repository, and analytics |  |  |
| Data logging and exportable analytics for EP ROI calculation |  |  |
| Customizable dashboard and team permission levels |  |  |

| Capabilities in Practice | Have capability | Importance |
|---|---|---|
| Key | ● Fully ● Partially<br>● Not at all | ● High ● Medium<br>● Low |
| Monitoring online threats or expressions of anger at specific location, organization, executive |  |  |
| Travel destination threat assessments |  |  |
| Vetting contractors (such as drivers, close protection, etc) at travel destinations |  |  |
| Surveillance or manned security at private locations (residence, office, venues) |  |  |
| Protection of digital assets/secure communications |  |  |

| Capabilities in Practice | Have capability | Importance |
|---|---|---|
| Key | ● Fully ● Partially<br>● Not at all | ● High ● Medium<br>● Low |
| Secure transportation on a daily basis |  |  |
| Monitoring personal reputation of the executive |  |  |
| Sending advance agents to unfamiliar locations deemed at risk |  |  |
| Close protection agents working with the executive on a daily basis |  |  |
| Close protection agents working with family (immediate and extended) of the executive |  |  |

## EP Travel Considerations

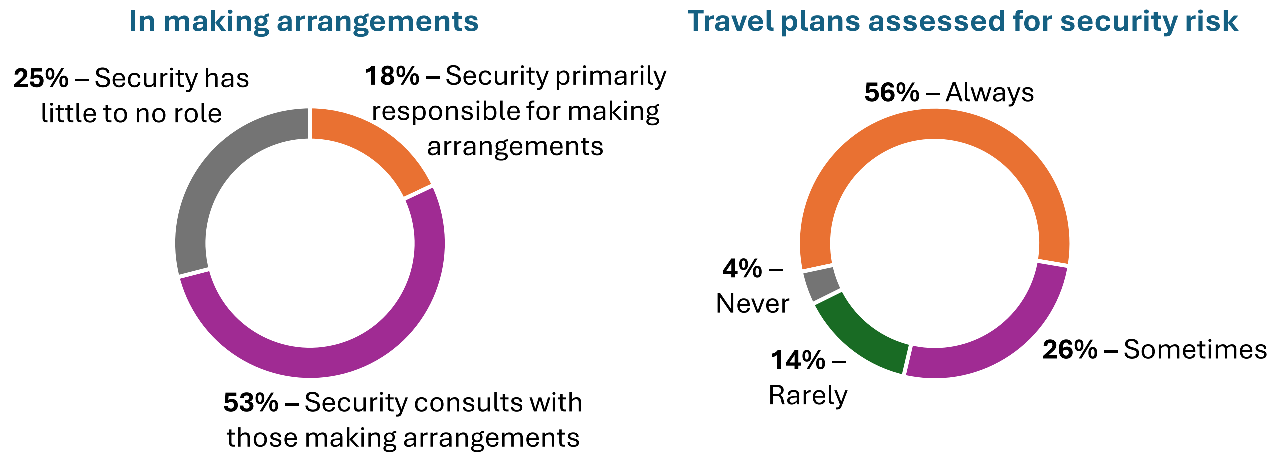
Because executives tend to be among an organization's most prolific travelers, executive protection and travel security have always been solidly linked. At most organizations, security consults with another department that actually makes the travel arrangements, however at 18 percent of organizations, security takes a more central role by making executive travel arrangements. Nearly a third (29 percent) of security departments have the disadvantage of having little to no roll in executive travel planning.

A pretty high rate of executive travel plans do not undergo any kind of risk assessment: 18 percent report such assessments are rare (14 percent) or never happen (4 percent). Another 25 percent perform executive travel risk assessments only sometimes.

When it comes to the protective measures organizations put in place when executives travel, organizations fall into three groups: those who are vigilant about the high degree of threat unpredictably when it comes to EP, so they tend to deploy resources most of the time (orange part of bar chart at right); there are those conscious of costs that let threat levels dictate the measures needed on a case-by-case basis (purple); and those that do not invest much in EP (gray).

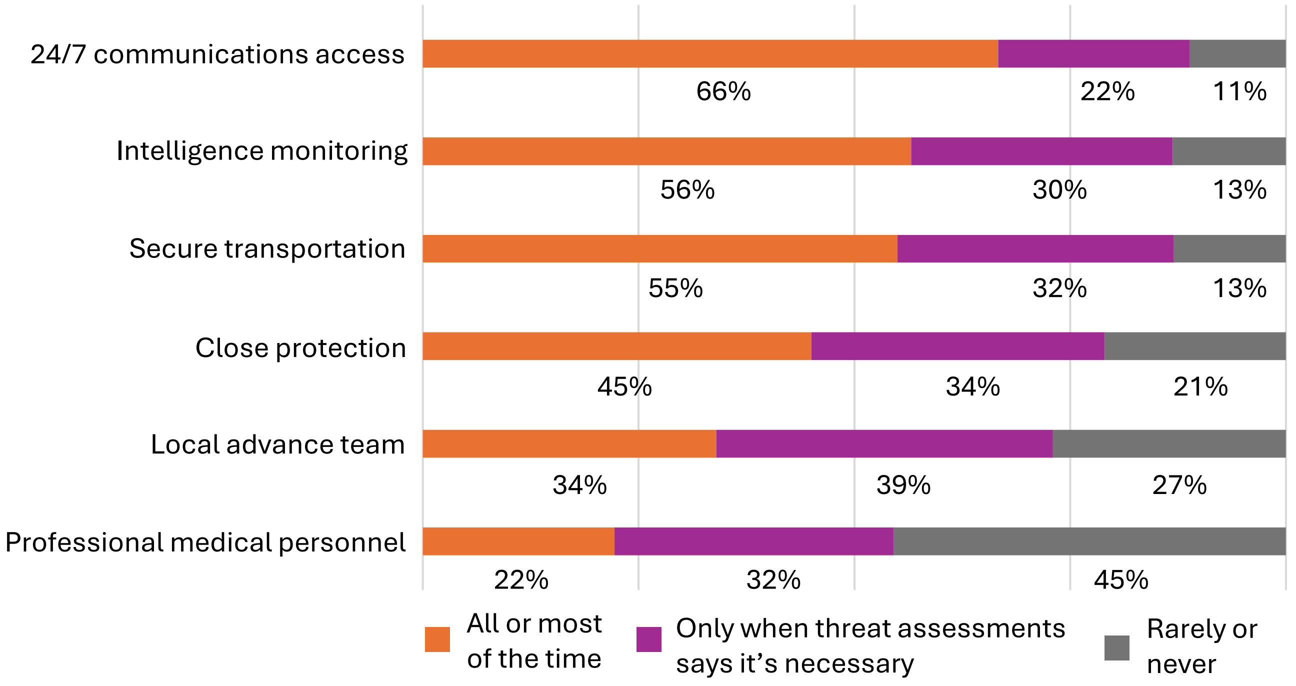
Overall, organizations are most likely to offer 24/7 communications access, secure transportation, and intelligence monitoring. They are much less likely to provide medical personnel.

## Security's Role in EP Travel Planning

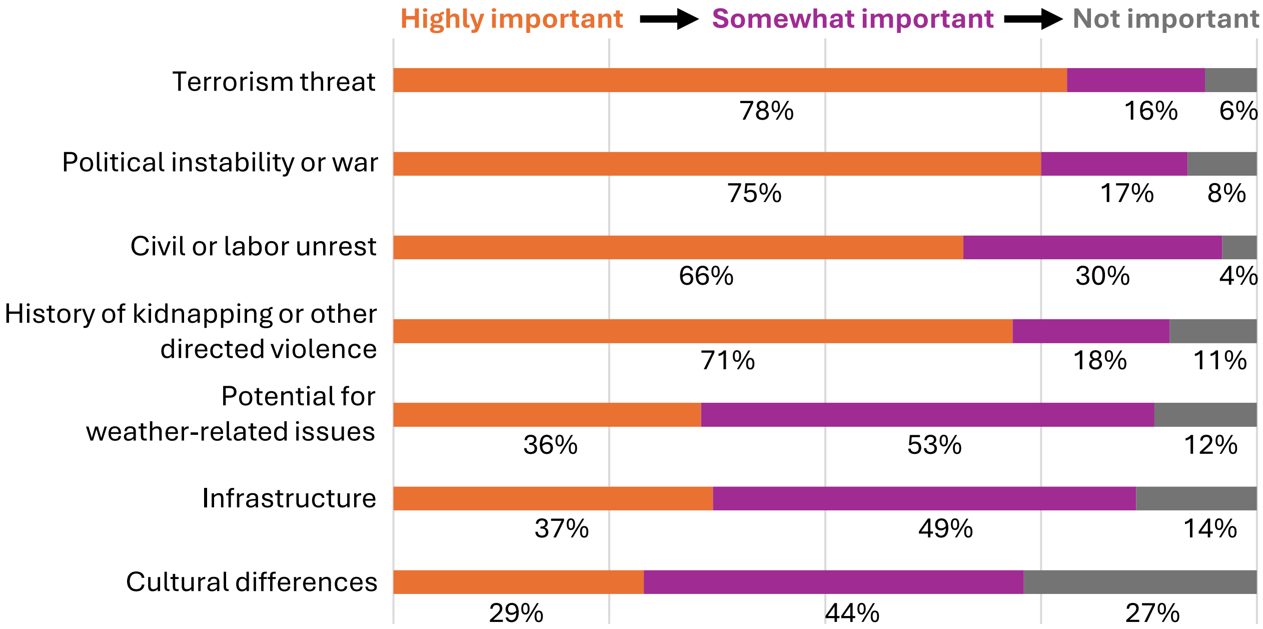

In making arrangements

Travel plans assessed for security risk

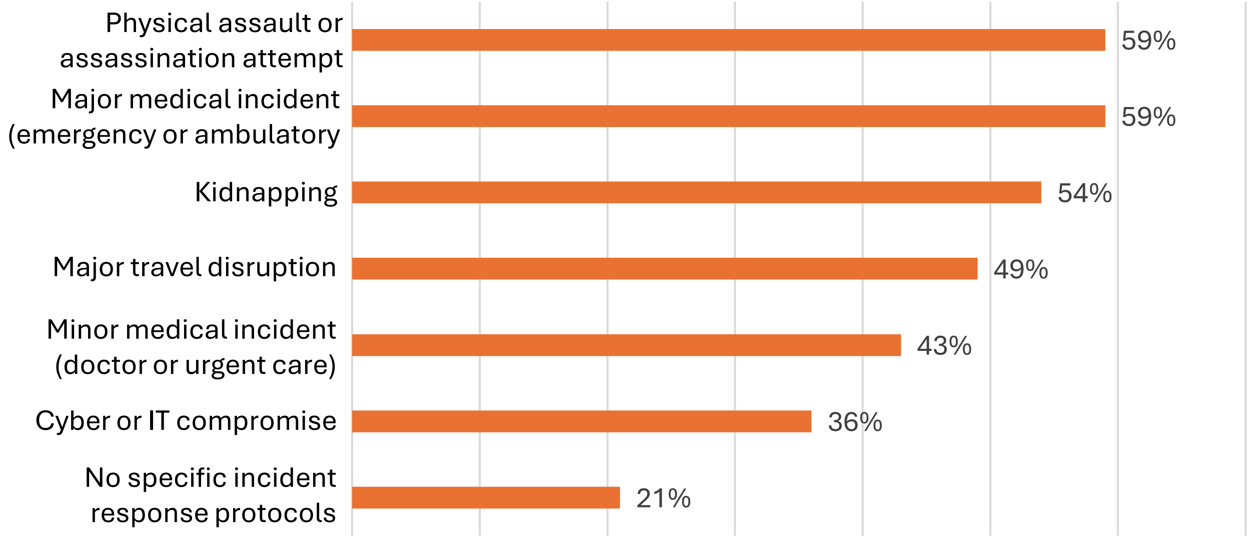
## Protective Measures Organizations Take for Executives on Travel



## Importance of EP Travel Threats



## Have Specific Incident Response Protocol



## Threats Executives Face While Traveling

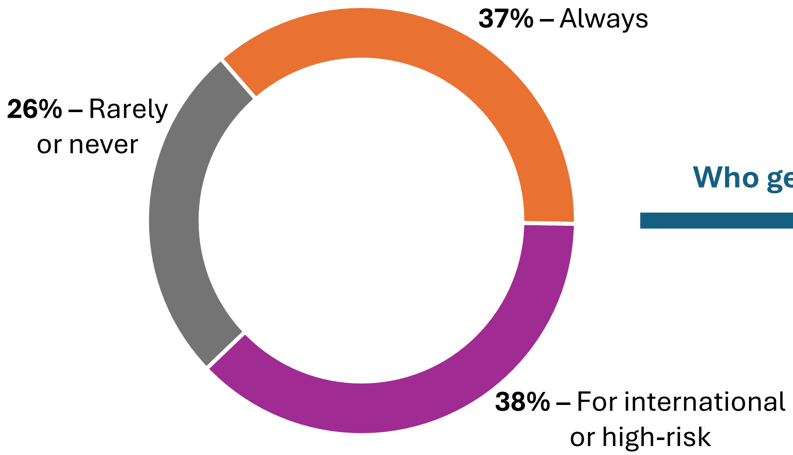
It is not surprising that the most unpredictable and violent situations—such as terrorism or kidnapping—were given the highest levels of importance from security executives. While weather and infrastructure issues could lead to dangerous situations, they are often less catastrophic and more predictable.

The low score of cultural differences is interesting and could reflect the extent of travel that executives do. If travel is mostly to modern, Western countries, then cultural differences will matter little. But culture can matter a great deal in other scenarios. Consultants were asked how well companies identify and prepare for these travel-related threats. All the threats scored similarly, except culture, which was the only below-average rating.

One-in-five security professionals reported that they do not have specific response protocols for EP-related travel incidents, which is alarming. Having a protocol in place would be invaluable if a major incident happened. More than that, while no organization could possibly develop protocols for all possible EP incidents that could cause disruptions, a protocol for one type of incident could readily be used and adapted for a different type of incident, likely saving valuable time in making decisions and taking actions.

## Safe Travel Briefings

The pre-travel briefing is an important part of executive protection travel security. A quarter of organizations do not provide such briefings, while the rest are evenly split between always providing them and only providing them for international travel or when the travel is to a high-risk location



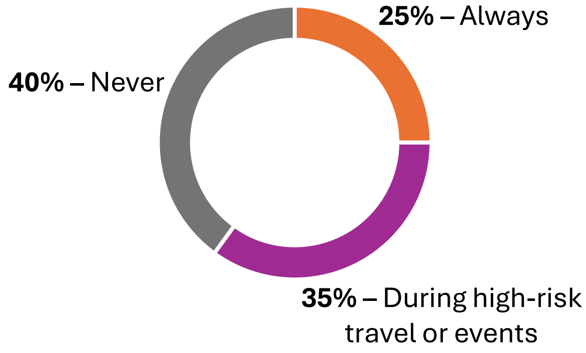
**Who gets these briefings?**

| | |
|---|---|
| **Executives themselves** | **82%** |
| **Personal assistants to executives** | **67%** |
| **Staff or family traveling with executives** | **46%** |
| **GSOC personnel (or equivalent)** | **36%** |

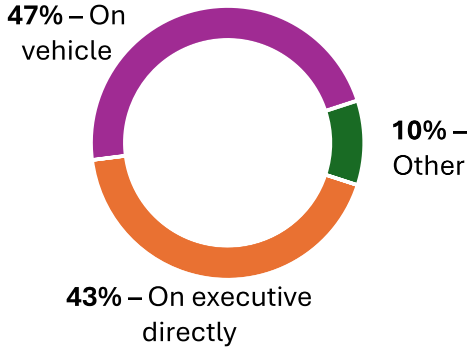
## Do You Know Where Your Executive Is?

To close out the executive protection travel security section, the survey asked about a specific technology: real-time location tracking.

### Use real-time tracking



### How is it deployed?



More than half of security professionals that chose other indicated real-time tracking was on both the executive and the vehicle. Most of the rest indicated real-time track was on the close protection team and/or driver.

## Executive Protection Training

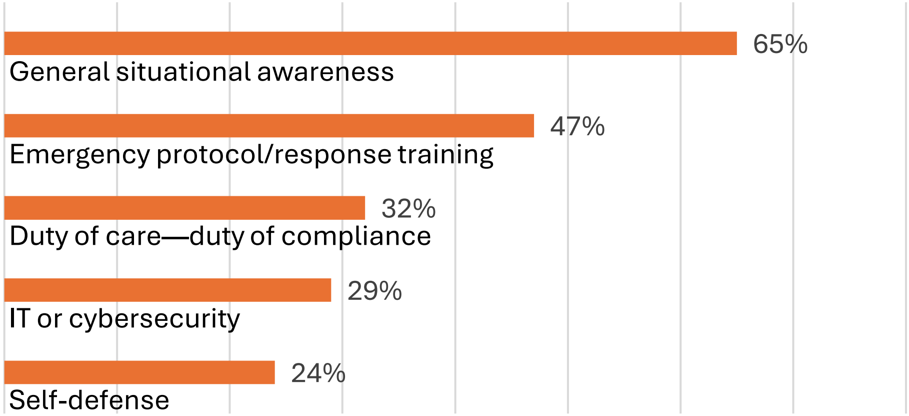
The survey examined three different kinds of EP training: scenario training, such as tabletops, specific training provided to EP personnel, and specific training for the executives themselves.

Only about 40 percent of security professionals report that their organizations conduct regular monthly (13 percent), quarterly (17 percent), or annual (12 percent) EP scenario planning. A quarter say they have never conducted such training, and the rest say it is on no set schedule.

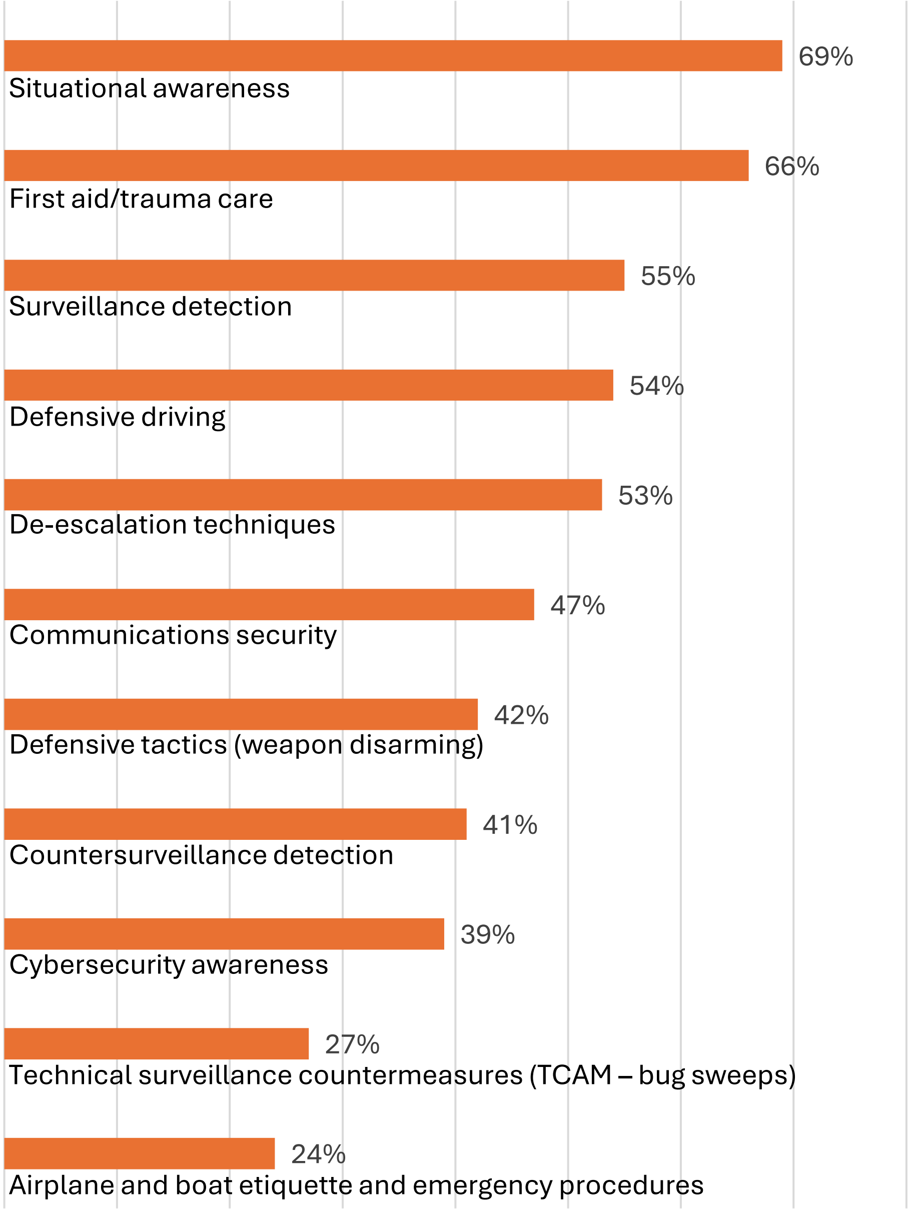
On a more personal level, situational awareness training was at the top of both the EP personnel and the executive lists. First aid or trauma training, surveillance detection, defensive driving, and de-escalation techniques round out the top five types of trainings organizations provide EP personnel—each type of training is provided by more than half of organizations.

For the executives themselves, only situational awareness training cleared the halfway mark, with nearly two-thirds training executives in the area. Nearly half (47 percent) trained executives on emergency protocols and emergency response, but it dropped off from there.

## Ways Executives Are Trained



## Ways EP Personnel Are Trained



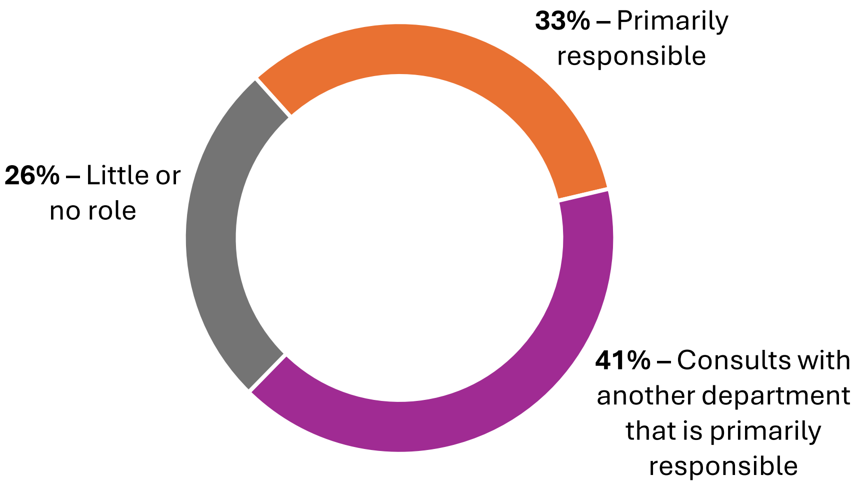
## Security as Reputation Managers

The reputation of corporate executives has not typically been within the scope of security management or even executive protection. However, the synergies between executive reputation and protecting that executive have developed quickly over the last several years.

First and foremost, the same social media monitoring and other OSINT tools used to scan for potential threats to executives can also be used to understand the perceptions of the executive among the public or key audiences. It's also not a stretch that the two are linked: How an executive is perceived can inform whether or not he or she is a target and what type of people might be doing the targeting.

Overall, 33 percent of security professionals report that security is primarily responsible for monitoring executive reputation. Bear in mind the possible biases of the survey—it was promoted as an executive protection survey, so it could, and probably does have self-selection bias from people with more advanced executive protection programs.

### Role of Security in Monitoring Executive Reputation



## Advice for Security Professionals

Interesting snippets from open-ended advice from the consultant's survey (slightly edited for clarity).

Many corporate security leaders misunderstand executive protection (EP) as merely a high-visibility security detail or bodyguard function. In reality, effective EP is a comprehensive, intelligence-led risk management strategy focused on prevention, discretion, and continuity.

Constant high threat levels risks less accurate interpretation of local security conditions.

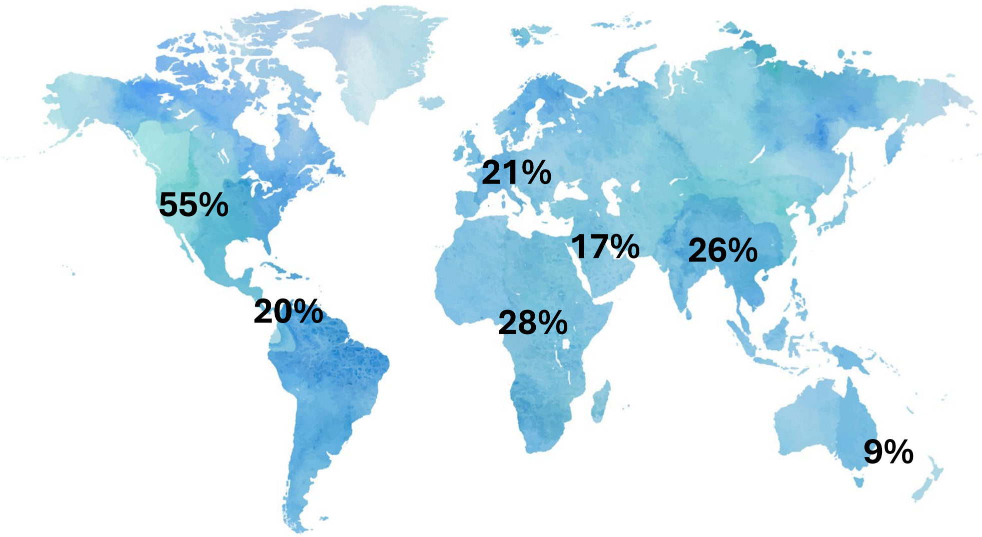
In reality, true executive protection is a proactive risk management discipline that blends intelligence, logistics, behavioral analysis, medical preparedness, and operational planning to ensure the principal's safety without disrupting their lifestyle or productivity.

EP is often misunderstood, which has led to underinvestment or poorly implemented programs. One common myth is that executive protection is only for celebrities or politicians. Reality: Corporate executives, especially those making high-stakes decisions or are involved in public-facing controversies, are at high risk.

Executive protection is more than proximity. It's strategic preemption, situational awareness, and business continuity rooted in subtlety and coordination.

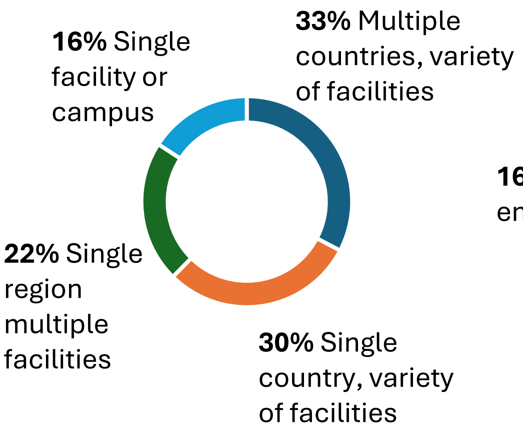
One of the key misunderstandings corporate security leaders often have about executive protection is underestimating how different the reality on the ground can be compared to what was initially briefed or planned. Being in the field directly with the client presents dynamic challenges and changing circumstances that can't always be anticipated from a distance. Unfortunately, GSOCs or command centers sometimes apply unnecessary pressure on field agents to follow rigid protocols, even when those protocols may not align with the evolving situation.

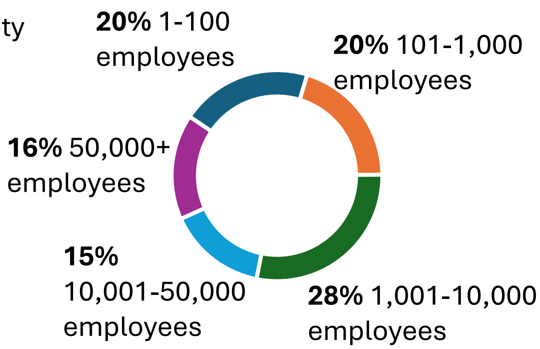
## Survey Demographics: Geographic Scope



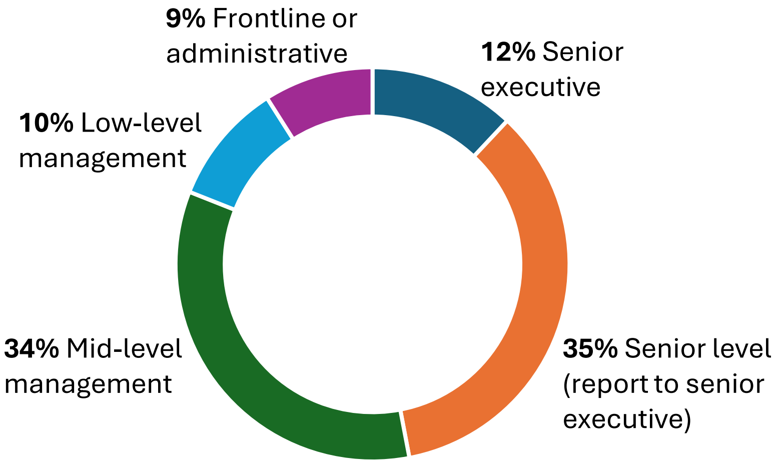
Participants were instructed to select all regions for which they had responsibility.

## Organization Size and Scope





## Position



## Sector

| | |
|---|---|
| Banking, Finance, and Insurance | 12% |
| Manufacturing | 6% |
| Oil, Gas, and Chemical | 6% |
| IT and Telecommunication | 5% |
| Healthcare | 5% |
| Defense and Intelligence | 5% |
| 19 others less than 5% each | 61% |

## Methodology

In the second and third quarter of 2025, ASIS International convened a small group of ASIS members and a representative from project sponsor Everbridge. This group put together a survey which was fielded in the month of July. The survey was promoted to ASIS members and customers via email, social channels, and ASIS newsletters. A total of 824 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 511 people answered the last question available to them in the survey, which includes 110 consultant surveys and 401 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 5 percent at the 95 percent confidence level. The margin of error for the consultant survey is plus or minus 10 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 an executive protection 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.

ASIS would like to thank the following individuals for their assistance in developing the Executive Protection Survey:

Kevin Palacios, CPP, PCI, PSP
Manager
HELPS Latam
Chair, ASIS Executive Protection Steering Committee

Darcy Leutzinger
Senior VP, Director of Security
United Wholesale Mortgage
Member, ASIS CSO Thought Leadership Committee

Lee O’Sullivan
Head of Global Security Operations
Everbridge

The project lead was Scott Briscoe,
Content Development Director, ASIS International.