SEPTEMBER 2018

Securing Our Corporate Leaders

A Survey of Executive Protection Practices

GROUNDWORK®

ASIS INTERNATIONAL®

Press:
media@groundworkglobal.com

Inquiries:
info@groundworkglobal.com

Executive Summary

All research begins with a question. Ours was simple: “What are organizations doing to protect their top people?”

Asking executive protection leaders to describe their programs, assess their preparedness to face the priorities they identified as their top challenges, and discuss what “best in class” means to them led to the emergence of a new perspective on the landscape of corporate executive protection within the broader EP space.

As in other segments—such as government and military executive protection—corporate EP is risk-driven, but it is more resource- and alignment-dependent. Corporate executive protection is not “black and white,” as many practitioners describe other types of protective programs; instead, it reflects great diversity in program design and development.

Based on survey results of more than 400 practitioners and interviews with more than 20 Fortune and Global 500 executive protection leaders, this study reveals the current state of corporate executive protection, ranks the top challenges and threats they face on behalf of their principals, and articulates eight best practices shared by programs identified as “best in class” by their peers.

Table of Contents

Executive Letter

The answer to the question of how organizations protect their top people is deceptively complex—in part because of the vast range of corporate environments that exist, and in part because of the absence of central governing bodies or regulation around executive protection.

Accountants have the Generally Accepted Accounting Principles (GAAP). Pilots require licenses to fly. Attorneys have the bar exam, and even teachers need certificates to enter the classroom. Yet most countries—the United States included—lack similarly clear, universally understood standards around executive protection practices and training.

That the parameters of executive protection are so vaguely defined only serves to emphasize the importance of open, active communication in the space. Nowhere is this more true than in the specific case of corporate executive protection. When considerations such as executive alignment and resource allocation may have as much impact on the protective strategies employed as the risk assessment itself, visibility into these trade-offs can offer guidance on how to make them as reasonably—and as safely—as possible.

In the spirit of Groundwork's broader mission to fully support our clients' needs, we embarked on the research explored here to better understand the landscape within which these executives—and those who protect them—operate, as well as how they manage the trade-offs associated with competing priorities. Certainly, we expect that the findings from this data will enable us to improve the quality and relevance of our services, as well as to better advise the clients who trust us with the security of their ground movements.

On a broader scale, we see this endeavor as an extension of our company's brand promise: guided by principle; grateful to serve; restless in our pursuit of excellence. Such excellence is only possible in an environment in which knowledge is shared and best practices are constantly discussed, debated, and improved upon. While this report is only one small step in this direction, we see it as an important component of our company's commitment to continually add value for our clients and to the industry at large.

We hope that the following exploration of the challenges facing executive protection teams, what modern EP programs look like, and what our data suggests as "best in class" practices leaves you with at least one takeaway that can be used to enhance your own organization's protective efforts—no matter your industry, company size, or location in the world.

Robert Dobrient
Founder & CEO, Groundwork

Chapter 1
Introduction

Senior leaders are among the most valuable assets of their respective organizations. It is this understanding that permits seven- and even eight-figure executive compensation packages, as well as the expectations and visibility that come along with them. Yet anecdotal reports suggest that protection around these key figures is often highly variable—even insufficient, in some cases. It is this discrepancy that led Groundwork, in partnership with ASIS International, to undertake a study asking how organizations protect their most valuable human assets. What does corporate executive protection (EP) look like in practice, in light of the visibility associated with top people? Which factors contribute to this diversity in program structure, and what do they mean for the larger question of executive protection best practices?

Defining best practices for protecting an organization's top people cannot occur in a vacuum; it is not possible without a broader understanding of the scope of services currently being rendered under the umbrella of "executive protection." Prior to this survey, initial research revealed very few existing resources that examined the diversity of corporate executive protection program designs. Yet, as both this research and conversations with security practitioners revealed, a tremendous range of EP programs exists. Some rely on traditional government models of security—which follow what one research participant described as "a maximalist approach" grounded in their statutory authority—while others embrace a more tech-savvy, intelligence-driven approach. Some do very little, while others are highly-developed, "best in class" organizations.

Evolution in the field overall cannot be overstated in this analysis. Not only is corporate executive protection a relatively new field—as compared to the long history of government and military executive protection—growth in the space has been driven in part by rapid advancements in technology. These influence nearly every aspect of security, within the context of executive protection. The impact of technology on EP has been so wide-reaching, according to several research participants, that it can no longer be decoupled as a contributing factor to best practice development; it must instead be treated as an undercurrent affecting every decision made by these programs.

Moreover, although defining best practices is a laudable goal, the intent of this report is not to attempt prescriptive guidelines that are appropriate for every one of the myriad situations and arrangements encountered by security practitioners. It must also be mentioned that the paper avoids diving into tactical detail about specific tools and practices, out of respect for the sensitive nature of the subject, as well as to protect the confidentiality of those professionals who graciously participated in interviews and surveys in support of this project.

Instead, the goals of this work are to:

- Describe the current state of corporate executive protection practice, as well as what drives variation among organizations.
- Offer a perspective on how prepared practitioners believe their EP programs are, and identify the most significant challenges they face.
- Explore commonalities found in "best in class" executive protection practices.

In doing so, this report attempts to define a "10,000-foot view" that offers both new security professionals and more seasoned protectors a previously-unexplored look at how corporate organizations are—from an organizational, operational, and planning perspective—securing senior leaders, board members, valuable clients, and others who meet their threshold for care.

RESEARCH METHODOLOGY

To achieve the intended outcomes described above, the paper presents a wide range of perspectives from across industries, organization sizes, and geographic scopes, using information gathered through a survey of security practitioners, as well as interviews with high-level security professionals overseeing their organizations' executive protection programs.

The 2018 EP Practitioner Survey

The 2018 EP Practitioner Survey was disseminated digitally over a two-week period in July 2018 and included 23 questions tailored to gain insight into respondents' experiences with and opinions on current executive protection practices and challenges, as well as their perception of industry-wide best practices. Sent to members and customers of ASIS International—which describes itself as "the world's largest membership organization for security management professionals"—respondents were screened for active involvement in their organizations' executive protection program. Of the 622 respondents, 461 responses were validated as active EP practitioners and analyzed for this report.

The survey was conducted anonymously, but initial demographic questions provided some understanding of the respondent base. While the survey was designed for U.S.-based practitioners, a small number (<10%) of participants hailed from international markets including Kenya, the United Kingdom, Canada, Mexico, the Philippines, Nigeria, and Bangladesh, among others. Responses reflect participants employed in organizations of various sizes, across a wide range of industries.

While it was designed for practitioners employed by commercial businesses across industries, the survey also engaged participants from education, nonprofit/NGO, and faith-based organizations, as well as those from governmental bodies, who have been included in this analysis given similarities in the nature of their operations. It also includes 184 respondents who self-identified as "Security, Professional, and Business Services," which has been understood to involve consultancies or firms offering some form of security services. For brevity, this industry segment is referred to as "security firms" throughout this report.

"All research begins with a question. Ours was simple: 'What are organizations doing to protect their top people?'"

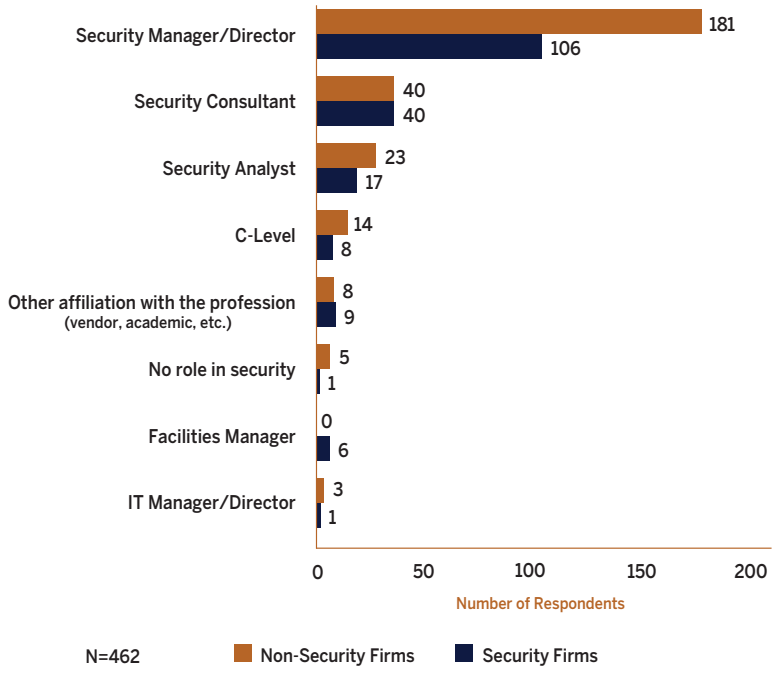
Survey Respondent Distribution by Industry and Organization Size

Industry Category	Employee Count <100	101-500	501-5,000	5,001-10,000	10,001-25,000	25,001-50,000	50,001-100,000	100,000+	Sum
Security, Professional, & Business Svcs	75	30	29	15	10	10	6	13	188
Government	4	7	9	5	9	5	5	8	52
Finance and Banking	2	4	5	7	6	2	4	5	35
Health Services & Pharmaceuticals	2	0	6	1	4	5	2	4	24
Manufacturing	0	1	5	5	2	5	3	3	24
Natural Resources, Mining, Agriculture	0	0	2	5	6	5	4	0	22
Consulting or Business Svcs	13	1	1	0	1	0	1	2	19
Education	4	2	5	4	1	0	1	1	18
Transportation, Utilities, & Industrial Svcs	2	2	5	2	3	2	1	1	18
Wholesale & Retail Trade	0	0	3	2	2	1	2	1	11
Non-Profit/NGO	5	2	3	0	0	0	0	0	10
Leisure & Hospitality	1	3	2	0	0	0	0	3	9
Faith-Based	4	2	0	0	0	0	0	1	7
Information & Research	1	0	3	0	2	0	0	1	7
Sports and Entertainment	0	2	0	3	1	0	0	0	6
Technology & Telecom	0	1	1	0	1	1	1	0	5
Conglomerate	0	0	1	0	0	1	0	1	3
Construction	1	0	0	0	0	1	1	0	3
Sum	114	57	80	49	48	38	31	44	461

Close to 20% of participants described themselves as the party responsible for their organization's executive protection program. Sixty-two percent of survey respondents described themselves as Security Managers or Directors, 17% identified as Security Consultants, 9% as Security Analysts, and 5% as C-Level (36% of these were leaders of security service firms). The remaining 7% reported to Facilities, IT, or were in other ways affiliated with the executive protection practice.

Survey Respondents by Role

Q: Which of the following most closely matches your job title?



As this was an anonymous survey, no subsequent engagement was undertaken and there was no opportunity to pursue follow-up discussion regarding their responses.

Industry Interviews

To supplement the insight garnered by the EP Practitioner Survey, phone interviews were conducted with more than 20 senior-level security executives from market-leading corporations, most in the Fortune or Global 500. The titles of these executives varied, but all were directly involved in leading executive protection programs, and most had served in multiple senior security roles. Over half of the interviews represented organizations with mature executive protection programs, many of which were recognized as "best in class" by their peers in survey responses.

Overview of Interview Participants

	Organization Size (Employee Count)						
Industry	<1000	1-5K	5-10K	10-50K	50-100K	100K+	Sum
Apparel	0	0	0	0	1	0	1
Aviation	0	0	1	0	0	0	1
Banking	0	0	0	0	2	0	2
Financial Services	1	0	1	0	0	0	2
FinTech	1	0	0	0	0	0	1
Healthcare	0	0	0	0	0	1	1
Hospitality	0	1	0	0	0	0	1
Insurance	0	0	0	0	1	0	1
Manufacturing	0	0	0	0	0	1	1
Payment Processing	0	0	0	2	0	0	2
Security	1	0	0	0	0	0	1
Technology	1	0	0	0	1	3	5
Transportation/Logistics	0	0	1	0	0	0	1
Sum	4	1	3	2	5	5	20

Interviews were conducted between July 2018 and September 2018, and participants were assured that their personal identities and the names of their organizations would be kept confidential. In the analysis that follows, these discussions have been used to provide greater context to survey results, as well as to offer real-world perspectives on how modern executive protection is carried out in organizations worldwide.

In addition, Gavin de Becker & Associates—highly-regarded experts on the protection of public figures with more than 40 years of experience in the field—participated in a review of the paper and shared additional insight on its findings.

Chapter 2

The Current Corporate Executive Protection Environment

Both survey and interview data make clear that the dialogue around corporate executive protection has changed dramatically in the last 10+ years as the industry has grown, the scope of its coverage has increased, and a greater number of people and organizations have joined the discussion. Understanding how today's corporate executive protection programs operate, therefore, requires a corresponding awareness of the environment in which they operate and how it has changed in recent years.

A MARKET PERSPECTIVE

Modern executive protection can be roughly divided into three segments: military, government, and the private sector. Private sector can be further divided into two camps: corporate, which this report defines as publicly-held companies and nonprofit or non-governmental organizations subject to scrutiny by shareholders, board members, and other stakeholders; and personal, which includes private companies, family offices, and celebrities or other high- or ultra-high net worth individuals whose security spends are not subject to disclosure. Though all share the same central tenets of executive protection, one survey participant explained that comparing these segments is not "apples to apples," given the breadth of goals and tactics required by each one. This degree of variance is evident in the way executive protection is executed across these different segments.

Within the government sector, for example, mandated protective services are provided for those involved in key matters of state or national security, including the President, Vice President, Secretary of State, and Director of the F.B.I., among a number of others. The government protects on a so-called "position level," meaning that protection is inherent in the job description. Yet, despite occupying a similarly high rank in the governmental hierarchy, Supreme Court Justices have a choice in the matter of their security. Though most recognize the need for protection as a responsibility of their role, what is notable is that they represent a rare exception in the government's protection program: principals who are afforded an option.

In the corporate sector—the focus of this study—this expectation is more often than not reversed. Although corporate executive protection has its roots in traditions of military and police protection, most corporate leaders still see protection as a choice, rather than a duty. The spectrum of practice that exists within the landscape of corporate executive protection is driven in large part by the inherent tension this choice creates.

"The design of any corporate EP program is ultimately determined by the risk profile of the principals, the availability of resources, and executive alignment."

Though EP programs across all segments are inherently risk-based, the design of any program is ultimately determined by the interplay of three factors, described in greater detail throughout this section:

- The risk profile of the principals;
- The availability of resources; and
- Executive alignment.

Three Factors Influencing Corporate EP Program Design

The single biggest distinction between EP segments called out in interviews was the balance between these factors. As one participant put it, in government, "security has a big voice." By contrast, "we spend a lot more time articulating why we're doing something and building the business case" in the corporate world, another shared. While government and military programs may seem to have endless resources, corporate executive protection must operate within the constraints dictated by these three key factors.

RISK PROFILES

Much of this variation can be attributed to the fact that government and corporate risk profiles are themselves very different. Where government protectees live with constant and known threats based on their roles, corporate leaders generally face fewer known threats. Rather, their threat profiles are based more on general risk, brand trust, and business continuity considerations. That said, those risks have increased dramatically in recent years.

As business travel emerges from what the Global Business Travel Association (GBTA) has called "The Era of Uncertainty" following the Great Recession, the organization now forecasts 7% growth in business travel spend in 2018, with continued growth between the years 2018-2022. Despite year-to-year volatility, this sits on top of a substantial period of growth in which business travel spend doubled during the 15-year period 2000-2015.[1] Not only are executives traveling more, they are visiting a broader range of places than ever before—and spending more time in them, as they chase the growth offered by emerging markets. Though organizations may not send their top executives to the highest-risk areas, the increasingly globalized nature of business often necessitates travel to these areas by someone in the organization, including those further down the corporate hierarchy.

At the same time, geopolitical instability and the democratization of terror mean that there are, effectively, more high-risk areas than ever before. For example, the 2018 Risk Map Report published by Aon in partnership with The Risk Advisor Group and Continuum Economics,[2] finds that "Overall political violence risk levels worldwide increased for the third year in a row, with 17 countries receiving increased risk ratings and only six receiving reduced risk ratings." Traditionally low-risk destinations are experiencing incidents as well—as highlighted by attacks in Manchester, Paris, New York and Boston, among others—increasing the executive protection requirements for areas once thought of as "safe."

Interview subjects spoke at length about what determines a principal's risk profile. The framework most use to evaluate risk and define mitigation tactics involves identifying potential threats, estimating the probability that those threats will occur, and assessing the potential impact (financial or otherwise) they could impose, should an incident occur. Security teams will then define thresholds between acceptable and unacceptable risk, at which point action should be taken to actively mitigate the risk.

Before evaluation of specific situations, events, and threats even begins, security teams must also understand the risk profile of their principal. Most research participants aligned quite neatly on what constitutes a "high risk" profile for a corporate principal. The characteristics they referenced can be summed up in four key vectors, which must be understood in context of the individual principal before planning around specific situations, events, and threats can begin:

- Influence
- Scope
- Sentiment
- Visibility

"Influence" refers to the principal's level of responsibility; for instance, a CEO typically faces greater risk than a mid-level manager.

"Scope" reflects the reach the organization—and, therefore, the principal—may have. A global organization usually has a higher risk profile than a local or regional one.

"Sentiment" considers whether the industry, organization, or principal are being discussed in a positive or negative light. Has the organization recently conducted layoffs? Is it financially stable? Has it faced a scandal of some sort? Has the principal made well-received comments or done something courageous or heroic? Does he or she engage in public discourse around politics, religion, or diversity issues that might provoke reactions? Any of these factors could increase or decrease the protection requirements of a given executive; though, as one interview participant noted, "it is the intensity of the feeling that is most critical—not whether it is positive or negative."

Lastly, "visibility" refers to how high profile a person, organization, or industry is. Some industries are simply more high profile than others. Consider the case of an oil and gas company executive—whose organization may be operating in volatile areas, as well as face animosity from environmental groups—versus one leading a company selling pipe fixtures.

Active social media participation and traditional media attention can also drive visibility at the personal level. Innocuous practices, such as sharing one's vacation or first day of school photos online can compromise sensitive information, transmitting it to millions of curious parties around the world instantly and creating vulnerabilities for those who would exploit this knowledge. Traditional media can achieve many of these same negative impacts by shining its spotlight on notable principals. That spotlight may be good, bad, or indifferent in nature, but for corporate executives—for whom a low profile is often key to successful risk mitigation—"any spotlight comes with consequences."

RESOURCE AVAILABILITY

Despite the strong case that more attention should be given to executive protection in light of these and other factors, investment in EP remains a challenge for many organizations. Commercial entities are still—and always will be—driven by their need to maximize earnings. Given the position of executive protection as a cost center, challenges in gaining the executive buy-in required for investment in non-revenue-generating activities are to be expected. "The return on investment (ROI) of the EP program is quite difficult to articulate to a company's leadership, as it is often challenging to prove the value of deterrence," described Gavin de Becker & Associates.

The cost of executive protection is a legitimate concern for organizations. Depending on how executive protection programs are structured, protective security details for individual principals must compete for the same pool of resources as other security needs, in addition the business priorities of other corporate functions, such as product development or human resources.

"The return on investment (ROI) of the EP program is quite difficult to articulate to a company's leadership, as it is often challenging to prove the value of deterrence."

– Gavin de Becker & Associates

PRINCIPAL BUY-IN

Even when resources are available, principals may reject the level of protection deemed appropriate by their EP programs. Of those survey participants who reported not having a structured executive protection program in place, the greatest share of respondents cited low or no perceived need as the causative agent. Some executives, for example, see having a security detail as an unnecessary hindrance which restricts the freedom of movement to which they are accustomed; one participant likened it to feeling as if they were "living in a cage," where simple things—such as opening vehicle doors for themselves—may no longer be allowed. Another related, "They want security, but they don't want anyone to know they have it and they don't want to see it." Principals may also resist protection because they:

- Want to avoid being seen as being wasteful of company resources.
- Assume that, since incidents have not occurred in the past, they will not occur in the future.
- Are humble (or naive), and believe themselves to be of little interest to potential bad actors.
- Fear that the optics associated with a visible security detail could be used to paint them and their organizations in a negative light.

One interview subject suggested that launching and growing a successful company often requires a bull-headed, "do what it takes" attitude; one that can be at odds with the more cautious nature required by executive protection activities. Principals may be more used to telling others what to do—not being told what to do themselves—which can create tension between the principal and his or her protective team.

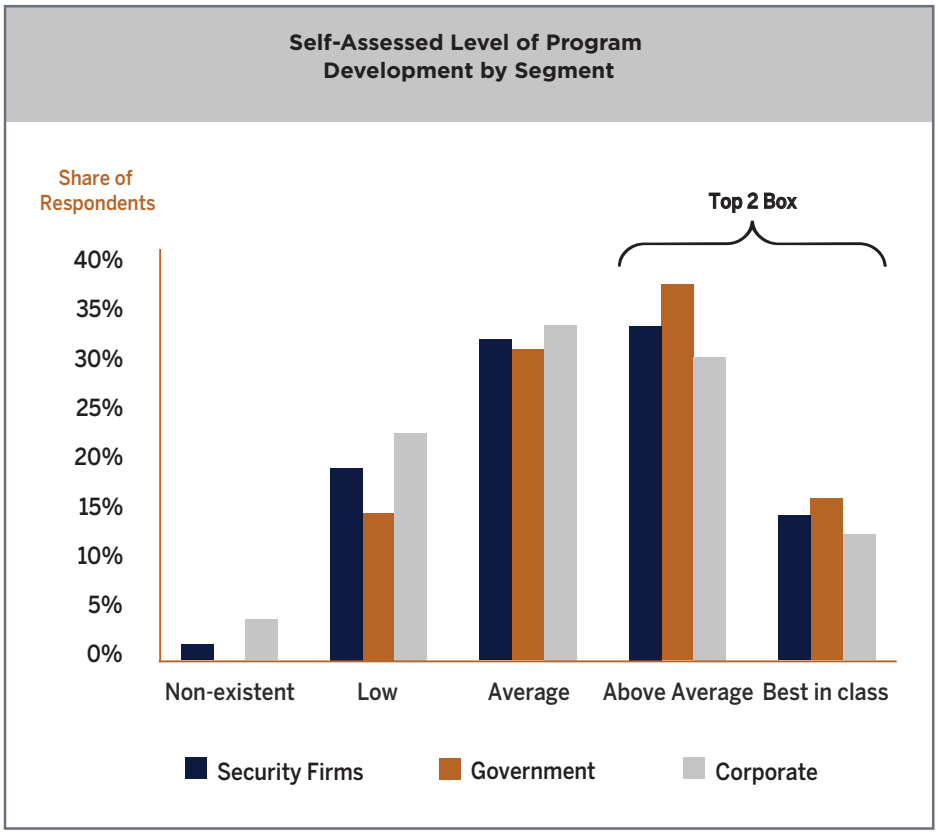
Chapter 3

A Closer Look at Today's Programs

Cognizant of the environment in which executive protection programs are operating, and while acknowledging that a protection program's tactical approach can only be determined in the context of its unique threat and risk evaluations, individual situations, and geographic factors, this study nonetheless attempts to draw conclusions on current practices among corporate executive protection programs in the spirit of understanding "big picture" trends. Despite this challenge, and the inherent limitations of a survey format, some clear insights can be gained with regards to the operations of today's EP programs.

EXECUTIVE PROTECTION PROGRAM MATURITY

Based on practitioners' answers to questions regarding the executive protection practices they employ, their threat priorities, and their self-described program maturity levels, it is clear that a significant degree of variance exists in executive protection program designs. While we attempted to approach this topic from a variety of angles, the survey question asking participants to self-assess their programs' maturity highlighted this phenomenon particularly well.



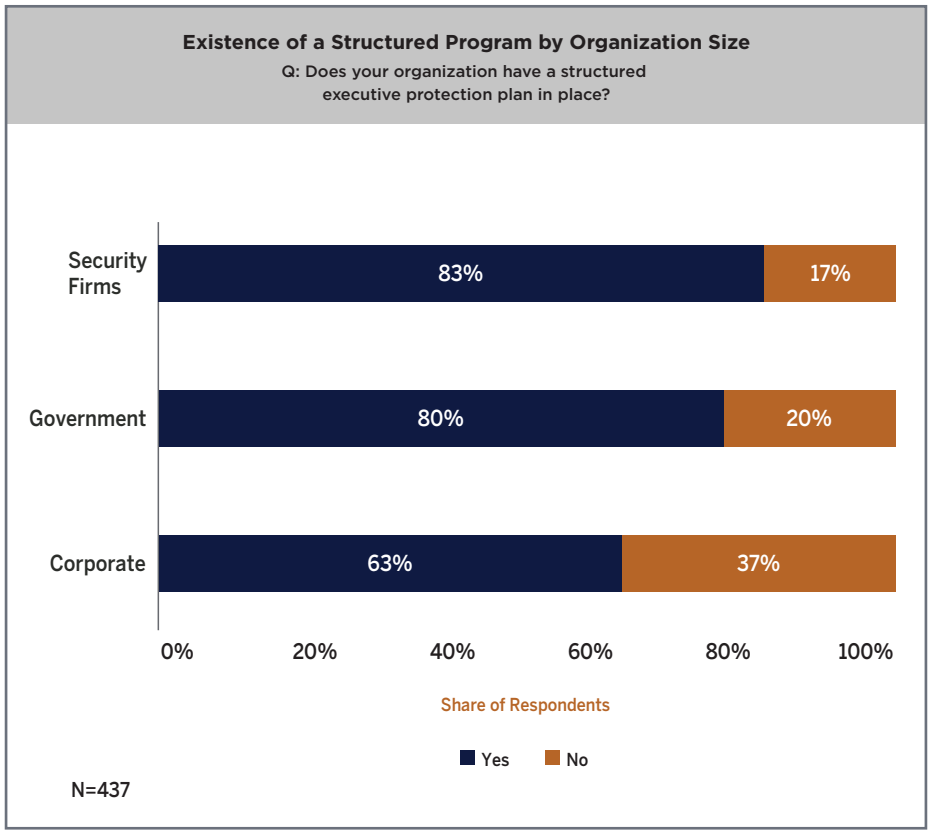
Across all respondents, 47% assessed their executive protection programs to be either "Above Average" or "Best in Class." Separating out responses from security firms and the government segment demonstrates a greater confidence on both of their parts: 54% of both groups put themselves in these top two categories, compared to 39% of non-security, non-government organizations.

One might expect larger organizations (as determined by number of employees) to self-identify as more mature than smaller ones, but the data suggests otherwise; no single size-based segment stands out as significantly more well-developed than another.

Interestingly, however, industry does seem to make a difference. More than 50% of respondents from the following industries identified their security organizations as "Best in Class" or "Above Average": leisure and hospitality (67%); natural resources, mining, and agriculture (55%); security firms and government (both at 54%); manufacturing (52%); and faith-based organizations (50%).

PROGRAM STRUCTURE AND ALIGNMENT

The existence of a structured approach to executive protection gives another perspective on an EP program's level of maturity. Two-thirds of non-security firms surveyed report having a structured approach to EP. Of security firms themselves, 83% agreed. While organizations of all sizes overwhelmingly report having a structured plan in place for executive protection (with 62-81% responding positively), mid-sized companies between 500-25K employees were the least likely to agree with that statement.

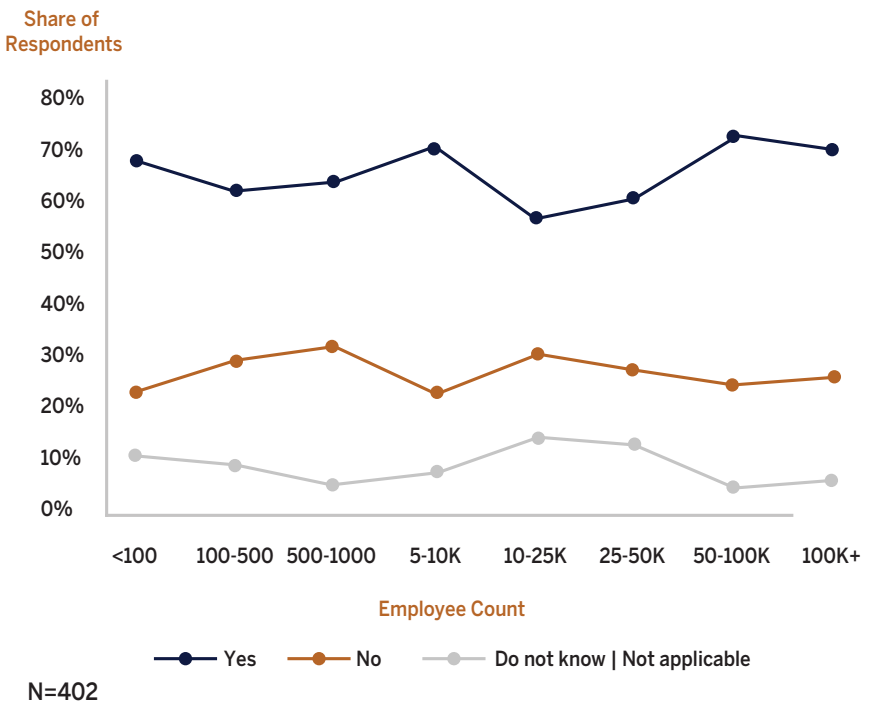


Of the 33% of non-security organizations indicating that their team did not have a structured approach to executive protection, 21% of respondents attributed the lack of attention to the perception of low risk within the company. Another 15% of responses noted that their program was in the process of being developed, but had not yet rolled out. Thirteen percent cited a lack of receptivity among executives, and 7% described their programs as informal and/or ad-hoc. The remainder pointed to factors such as a lack of resources or personnel to lead the effort; companies and security programs in transition including start-ups, those restructuring, or recent program discontinuation; or internal reliance on a market-by-market approach.

Alignment of executives and their support teams provides yet another perspective into the level of development of executive protection within organizations. Excluding security firms, 61% of survey respondents report alignment between principals and the EP team regarding the level of protection needed. Thirty-one percent indicate no alignment, while 8% indicated that they did not know the degree of alignment (or that it did not apply to their organization).

Principal Alignment by Organization Size

Q: Are the principals in alignment with the security team on the level of protection needed?



N=402

Buy-in from principals' support teams—for example, their executive assistants or travel managers—reflects similar patterns. Sixty-two percent indicate alignment, 32% claim a lack of acceptance, and 6% responded that they did not know. Among both groups, alignment appears to be agnostic to organization size, though three industry segments reported staff alignment at or below 50%: technology and telecom (only 20% responded positively); conglomerates (33%); and wholesale and retail trade (50%).

RESOURCING SOLUTIONS

Moving beyond the topic of program sophistication, the survey also addressed more straightforward questions regarding common EP practices, beginning with the issue of resourcing. When sourcing human capital for executive protection, private organizations have several options: building protective talent in-house, outsourcing the need to a third party, or leveraging third parties but bringing them in-house as embedded staff.

Research participants discussed a range of pros and cons associated with working with each type of resource; most notably that vetted, trusted third parties can supplement internal resources in distant markets or during large scale events or activations. Several interviewees noted that—given the significant range of travel destinations requiring support—maintaining and deploying internal full-time employees (FTEs) simply is not feasible in all situations. Working with contractors can also provide EP teams with access to specialized skills. For example, one interview subject mentioned bringing in a team of experts to conduct bug sweeps before each Board of Directors meeting. Others emphasized working with third party vendors to audit and manage a principal's personal (as opposed to professional) digital footprint as an opportunity to maintain some semblance of privacy between the principals' professional and personal lives.

Embedded contractors were also described as a great way to get to know a potential full-time hire before extending an offer of employment. However another participant pointed out that embedded agents, who are typically newer to the team and less sure of their future, may be more likely to make exceptions for executives' requests than an internal resource. As most survey responses indicate, though, in-house staff are far and away the most popular option—if the team can afford them. "I always prefer my own people," was a common response shared by interview participants.

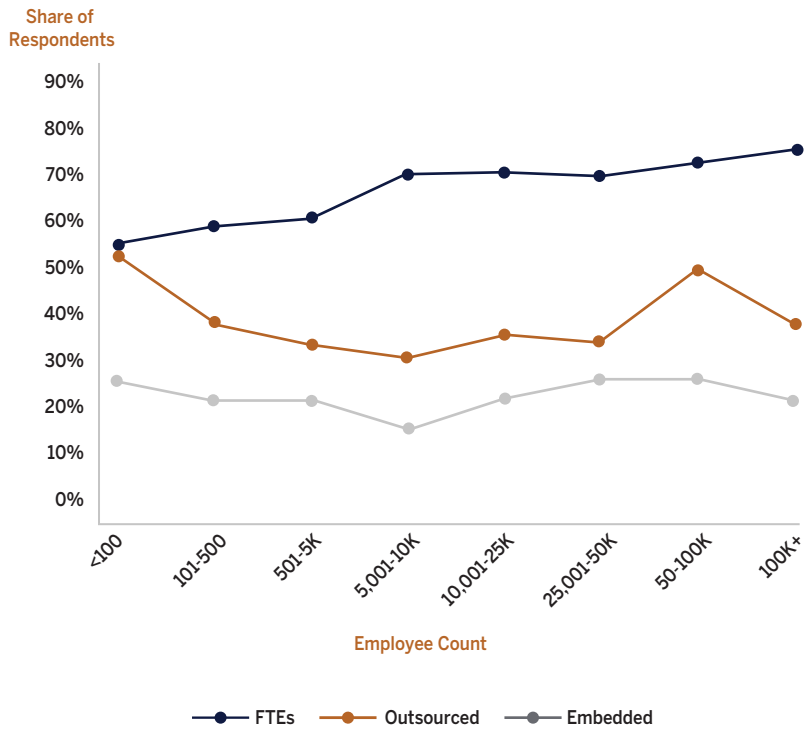
Though situation and location play heavily into resourcing decisions, only 6% of non-security organizations utilize all three resource types. Of those using only one type of resource, 61% relied on in-house people, 24% outsourced their EP function, and 15% utilized an embedded resource.

Across all 435 responses:

- 69% report using internal FTEs, 41% make use of outsourced contractors, and 23% leverage embedded resources.
- 72% use only one type of resource, 22% use two, and 6% use all three resource types.

Type of Resources Used by Organization Size

Q: Which of the following describes the resources in your executive protection program? (Check all that apply)



N=462

RATE OF ORGANIZATIONAL CHANGE

Survey respondents commented further on the rate of change within their protection programs. Forty-six percent reported that the security protocol around their organization's key people had changed in the last 24 months; 54% said that it had not. While these shifts were attributed to a wide variety of factors, 14% pointed to company growth or a heightened/lessened public profile, while 13% were due to executive request. Other factors cited, in no particular order, include:

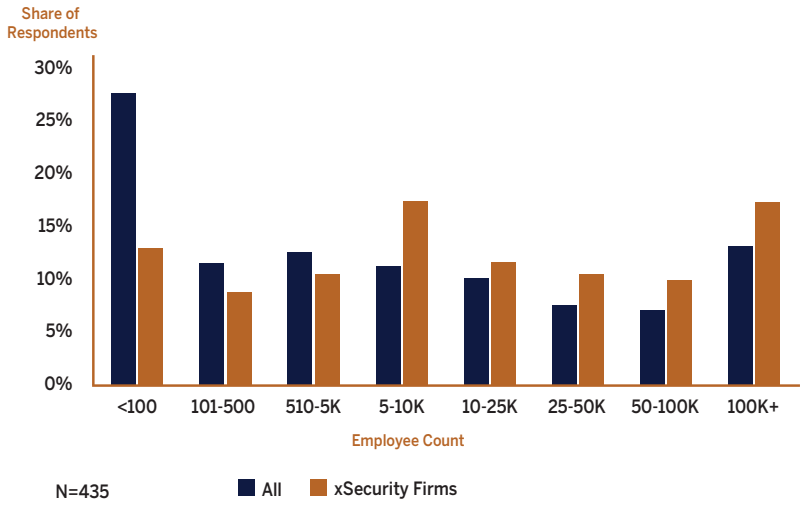
- Increasing threat levels, including terrorism
- Protests and the current political climate
- Active shooters
- Local crime activity
- Kidnapping
- Improved engagement of the security team
- New initiatives
- An increase in travel
- New legal requirements

ASSESSING OVERALL LEVELS OF EP PROGRAM SOPHISTICATION

One intent of this analysis was to explore which factors might help predict an EP organization's level of sophistication and overall development, potentially to define reasonable benchmarks for companies meeting certain descriptions. Would certain industries, sectors, or company sizes correlate with greater levels of preparedness than others? Could causal factors be determined? While the answers to many of these questions remain unclear at this time, several options can be eliminated.

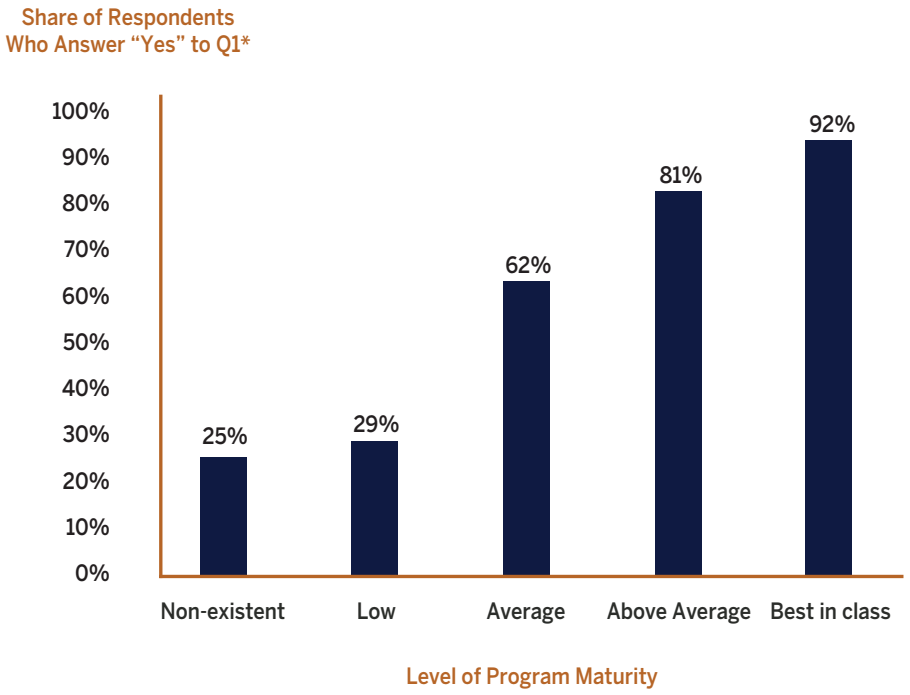
Organization size does not appear to drive program sophistication. As noted earlier, the analysis of this dataset shows no relationships between size and self-reported maturity. Feelings of preparedness also demonstrated no clear pattern when compared to organization size, until reaching enterprises with 25,000 employees or more. In these cases, preparedness remains consistently in the high positives, with 50-70% of responses in agreement.

Self-Assessed Level of Program Development by Organization Size



The existence of a structured EP strategy did reflect an interesting phenomenon: that the smallest and the largest organizations surveyed were more likely to claim a structured approach to EP. Mid-sized organizations from 1,000 to 25,000 employees reported the lowest likelihood of having a formal structure in place, which could be an indicator of confusion as companies outgrow their original EP strategy.

Level of Program Maturity Increases With Principal Alignment



N=261

* Q1: Are the principals in alignment with the security team on the level of protection needed?

One particularly interesting finding showed that levels of maturity do appear to scale with executive alignment, which begs further questions. If the level of development of an executive protection program improves with executive alignment, would the data reflect the same relationship when financial success, rapid growth, or organizational health facilitates the investment of necessary resources, or when clearly defined risk profiles and threat assessments dictate the need for higher levels of protection? Further exploration is clearly warranted.

Chapter 4

Facing Current and Future Challenges

The need for corporate executive protection has never been greater, yet executive buy-in can be limited, and resource allocation may fall short of what security professionals desire. The strategies employed by organizations to balance these competing priorities can contribute to the success of their programs, but are not the only factors that influence overall preparedness or satisfactory program outcomes. Many additional elements play a role in how EP programs are structured and how they can successfully prepare to address their challenges.

The duty of care conversation has helped move discussions around threat management forward by driving awareness of the personal safety risks faced by employees and by better articulating the financial cost of failing to adequately address those risks. In fact, 63% of survey respondents called out duty of care as a significant stimulus behind the development of risk management programs. But despite ongoing conversations around duty of care, few organizations have fully embraced a government-style approach that mandates a comprehensive, 24/7 protection program.

According to several interview subjects, the tipping point needed to resolve this challenge, unfortunately, is often an incident—whether directly experienced or learned about second-hand—that provides the momentum required to push previously-made proposals over the finish line. Waiting for an incident to prompt investment in corporate executive protection is, of course, a reactive approach; one over which many interviewees expressed frustration. Progressing to a more proactive approach requires movement on many fronts, the first of which is a better understanding of current corporate executive protection priorities.

One of the most fascinating lines of questions addressed in this research involved the challenges faced by executive protection teams, both tactical and strategic. To distinguish between the two, survey respondents were first asked to prioritize what they considered to be the biggest threats facing the executives under their watch. They were then asked to consider the longer term challenges standing in the way of their success in terms of the next priority on their broader EP agenda, be it strategic, organizational, capability-related, or threat-specific.

While these questions are admittedly difficult to think about without understanding the context in which they exist, a top of mind review nonetheless converged on a short list of broadly applicable topics.

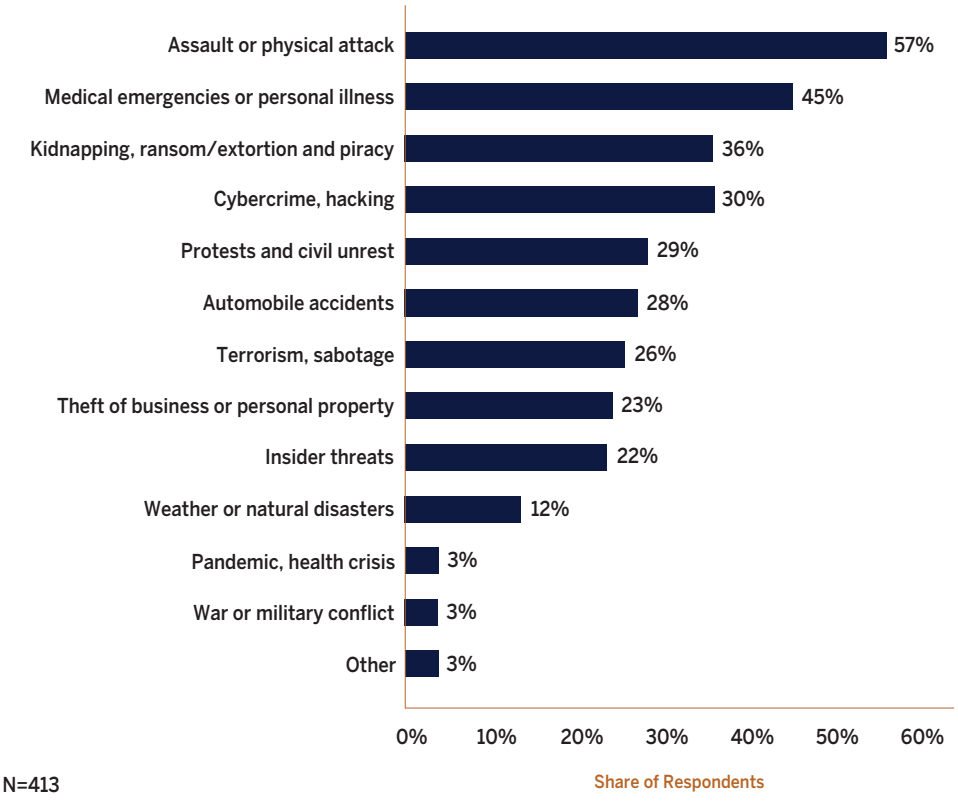
“63% of survey respondents called out duty of care as a significant stimulus behind the development of risk management programs.”

THREAT ASSESSMENT PRIORITIES

When it comes to immediate threats to the safety of their principals, both at home and away, practitioners' top three concerns reflected both mundane, commonplace risks and more acute, targeted threats. Issues arising from being caught in the wrong place at the wrong time were less frequently prioritized by survey participants.

Immediate Threat Priorities

Q: What do you believe are the three biggest threats facing the safety and security of executives today, either when traveling or when in their home markets? (Please select three)



N=413

Nearly 60% of respondents included physical attacks on the principal in their top three perceived risks. One European director drew attention to acid attacks as a more recent variant on his radar. Interviewees clarified that in addition to traditional assault, they also put attempts to embarrass principals in this bucket, with pie attacks being a commonly referenced example. "Reputation attacks," specifically, was written in by several survey participants as a top priority and might have emerged as a larger trend, had it been included as a standalone option in the initial survey.

Medical emergencies were the second most commonly selected concern, with 45% of professionals putting the issue in their top three. As one articulated, medical emergencies are a priority both at home and when they travel, particularly because standards of medical care and proximity to facilities vary so greatly from one country to the next. Another noted that the age of many executives, as well as the stress of their roles, made cardiovascular events a regular cause for concern. The issue is magnified by Zurich American Insurance Company claims data,[3] which found that "medical emergencies constitute more than 60% of incidents during business travel." Gavin de Becker & Associates confirm this finding, "To provide context to the criticality of this issue for EP work, our firm's 750 Protectors accessed their medical kits on more than 20 occasions last quarter and did not draw their weapons a single time."

Several respondents reported prioritizing the use of security personnel—whether in-house or outsourced—with emergency medical training as a strategy for mitigating the potential impact of these incidents. Gavin de Becker & Associates continue, "An effective EP program will have a baseline medical training requirement for all team members (CPR, First Aid, and AED) and will mandate quarterly or semi-annual training in these perishable medical skills." "Perishable" is a key word here, as it is important to emphasize that medical training must be continually revisited to remain relevant and useful.

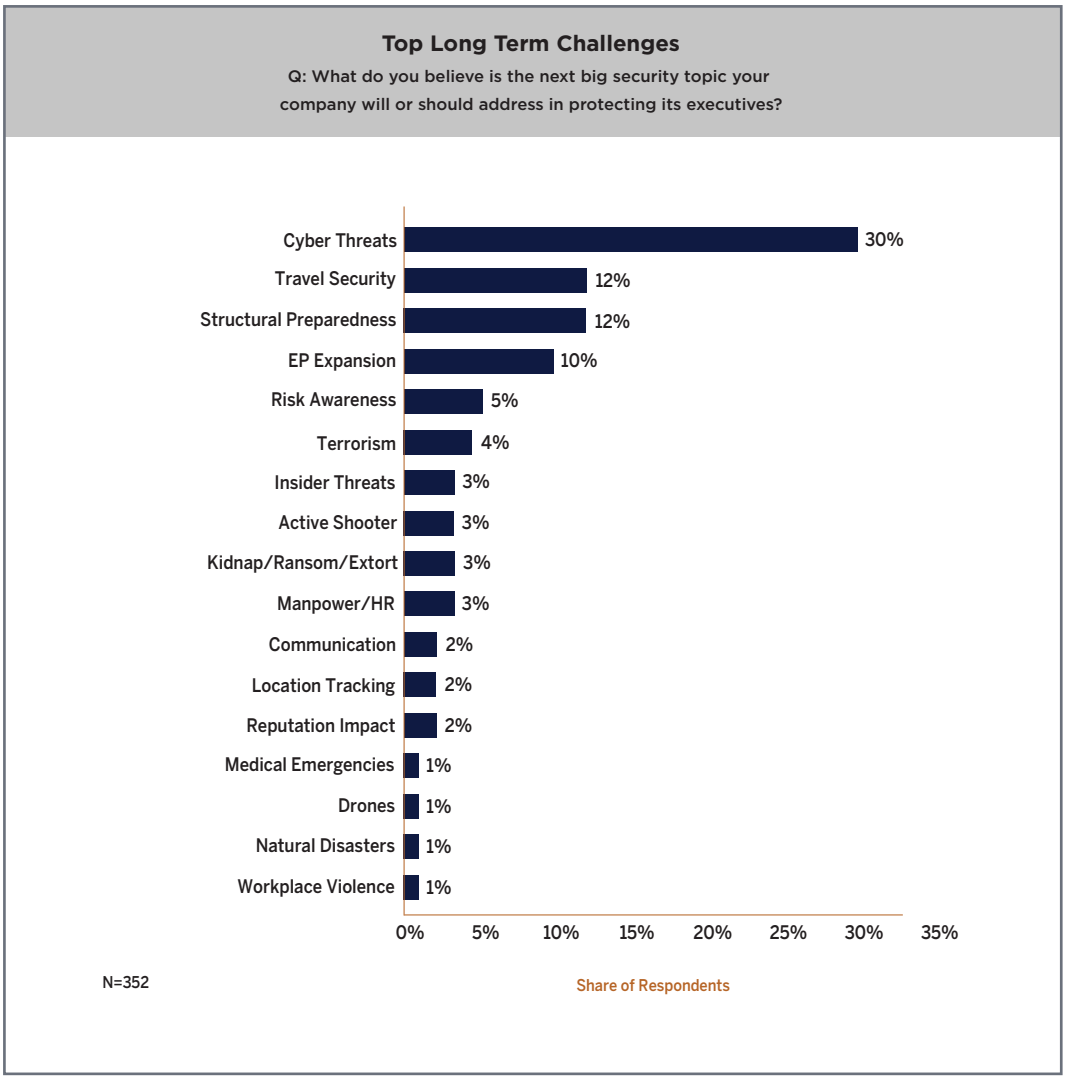
Tied for fourth place in terms of mentions were kidnapping, ransom/extortion, piracy (especially when executives travel abroad), and cybercrime and hacking; over one-third (36%) of respondents prioritized each of these threats. While cybercrime—discussed in greater depth in the next section—is understandably a trending topic, a lack of information around executive kidnapping made its presence so high on the list a bit of a surprise.

As organizations tend to avoid public acknowledgment of kidnapping incidents, their probability is difficult to ascertain, though the Bureau of Consular Affairs at the U.S. State Department estimates that as many as 60-70% of international kidnappings of U.S. citizens go unreported.[4] AIG estimates this number may be closer to 90%.[5] That said, its inclusion in these ranked responses indicates that the potential impact of losing a senior leader to threat actors may be enough to merit significant attention. One VP interviewed referenced salary disclosures in SEC filings: "It's not hard to imagine a $2 million ransom being paid when they know exactly what he's worth to the organization."

PROGRAM DEVELOPMENT PRIORITIES

A broader discussion around the challenges faced by executive protection teams began with an open-ended survey question asking, "What do you believe is the next big security topic your company will or should address in protecting its executives?"

A deep level of consideration was evident across the more than 300 answers received, which paved the way for thoughtful conversations in discussions with interview subjects. Subjects mentioned covered an incredibly broad range, reinforcing the idea that every company faces its own specific set of concerns and that there is no one universal risk profile. Take, for instance, the example of weaponized drones. For a company hosting a significant number of outdoor activations, the threat of drones is highly relevant; for another, drones may not even make the list.



When aggregated into related topics, the top four priorities detailed by research participants, in order of mentions, include:

- Cybersecurity
- Travel risk management
- Organizational operations and structure
- Program expansion

Cybersecurity

That cybersecurity appeared near the top of the lists of both the immediate threats and the longer-term horizons for security professionals suggests the magnitude of the problem, the rate at which it continues to evolve, and the difficulty associated with managing it. But it must be noted that the term covers an incredibly broad set of topics, many—if not most—of which, various information security teams (rather than physical security teams) may be responsible for addressing. Regardless of who owns responsibility for cybersecurity, though, many horror stories demonstrate the cross-departmental impact cyber threats can have.

The following specific cybersecurity-related topics came up in comments and interviews:

- Digital footprints
- Social media
- Identity theft
- Home networks and internet-enabled appliances
- Cyberstalking and cyber harassment
- Hacking and data protection
- Network intrusion detection and prevention
- Travel-related vulnerabilities
- Social engineering and fraud
- Device security
- SIM card swapping

The critical nature of educating executives—and their families and domestic staff—on appropriate digital protocols was also a recurring theme under the topic of cybersecurity, given that the threats evolve so quickly and the stakes have become so high. At the office, network systems can mitigate the impact of non-compliant behavior. But at home, on the road, or in a hotel or other quasi-"safe" facility, security teams must rely heavily on executives' own awareness and behavior to reduce their risks.

One interviewee commented, "the biggest threat to executives isn't physical; it's their devices." With their access to trade secrets, corporate plans and networks, they are prime targets—especially when traveling, and especially because they often lack awareness of how big the threat truly is. Corporate espionage has long been a concern, but with state and other actors employing new techniques that enable the wholesale access to—and the monitoring of—devices and networks, the scale of such activities has become unprecedented.

A number of practitioners pointed to digital footprints as another prime example. Even with added education around how to manage their cyber profile, many executives still struggle—particularly when they have multiple online personas. Complicating the situation is the issue of privacy and the fact that, in addition to their professional profiles, executives have a personal digital footprint, and may be unreceptive to their corporate security team monitoring their private online life and that of their families.

Home networks offer yet another vulnerability, especially as the Internet of Things (IoT) grows. Home networks may not be maintained to the same standards as dedicated IT teams put into office networks, despite the vulnerabilities this creates.

Insecure "smart" home devices—such as thermostats, baby monitors, and other appliances—exacerbate the problem. One participant shared a story of a test in which an organization parked an analyst on a laptop in front of an executive's residence. Within the hour, the analyst had hacked the executive's home network and gained access to sensitive information stored there. His point was clear: it may be easier to rob someone from thousands of miles away on a laptop than it is to physically break in and access a hidden, locked file cabinet.

Travel Risk Management

Nearly every interview touched on challenges associated with employee travel, regardless of the relative level of risk associated with the destination or the seniority of the employee involved in the travel. Travel security was also the second most common challenge prioritized by survey respondents, largely because of its logistical complexity. One professional explained, "the biggest risk our team faces is logistical stuff. Secure transport, that's my biggest fear. Medical issues are the second thing I look at. The logistical things are the issues you're most likely to face." Another put it simply: "Amateurs talk tactics. Professionals talk logistics."

One participant, who averaged 270 nights on the road with his principal, mentioned unreliability and inconsistent service delivery as deal-breakers. In particular, he expressed concern around wondering if pre-arranged vehicles would show up, if the hotel advance been done the way he needed it, and over being able to locate the nearest and most preferred hospitals, should an emergency arise. Another emphasized the logistical nature of his role, saying, "If he wants to go to Mars, it's my job to get him there safely."

Secure ground transportation was called out most often as a baseline requirement for travel—which was, perhaps, unsurprising, given that 28% of survey respondents chose auto accidents as a "top three" threat, resulting in its placement as the sixth most highly-rated risk. Even in organizations with comparatively light protective coverage, one practitioner noted, "at the very least, I make sure they have a security driver when they travel." Data from the World Health Organization supports this practice, finding in 2013 that more than 1.2 million people die each year in automotive accidents, while another 20-50 million people suffer non-fatal injuries.[6] Further, according to U.S. Department of State data shared in the Center for Disease Control (CDC) Yellow Book 2018, "road traffic crashes are the leading cause of injury deaths to U.S. citizens while abroad."[7]

The case for secure ground transportation was frequently made by interviewees in the context of international travel where armored cars, mentioned by several survey participants, may be a necessity, and where the varying regulations and other issues regarding the resolution of auto-related incidents may up the ante for traveling

"The biggest risk our team faces is logistical. Secure transport, that's my biggest fear. Medical issues are the second thing. The logistical things are the issues you're most likely to face."

executives. That said, many interview participants made the case for round-the-clock drivers on a domestic basis as well: compared to a security driver, one articulated, executives "are all distracted drivers." He expanded that—even on the weekends, when they just want to enjoy driving their own car—if a principal is mentally preoccupied thinking about an upcoming deal or talking on the phone, it would be a disservice to let them drive themselves. Making sure these drivers, whether internal or outsourced, were covered by strong NDAs and confidentiality agreements served the complementary purpose of enabling executives to use transit time productively for sensitive tasks, according to another interview subject.

Organizational Operations and Structure

The third most frequently identified type of improvement EP professionals planned to make were what can be considered foundational improvements, including structural, cultural, and capability-related changes. Specific initiatives cited include:

- Strengthening organizational policies
- Standardizing practices and the consistency of their application, including "to ensure that standards are maintained as principles change"
- Enhanced insurance
- Establishing a Security Operations Center (SOC) or fusion center capability
- Strengthening business continuity and crisis management plans
- Changing the view of EP within the organization broadly
- Eliminating principals' resistance to the program
- Building out threat intelligence capabilities to enable the use of "less brawn…more brains"

Training also came up frequently in these responses, particularly with regard to training executives in risk awareness, certification of agents, battling complacency, and identifying better opportunities to provide their people with real-world preparation.

EP Program Expansion

According to several interview participants, corporate executive protection efforts often start small with a single effort around a Chief Executive and expand from there as need, support, and resources become available. International travel or sizable public events often constitute the first ad-hoc needs, but once a principal experiences the logistical benefits a detail can provide, the journey to building support for a program may accelerate.

Nonetheless, the leaders we spoke to were vocal about the need for more than off-and-on or "business hours only" protection. Those advocating for program expansion were primarily focused on adding depth to the program; often through the use of full-time driver(s) and 24/7 coverage for their principals. Armed escorts and residential monitoring of primary and subsequent properties were also called out in the survey as initial expansion opportunities.

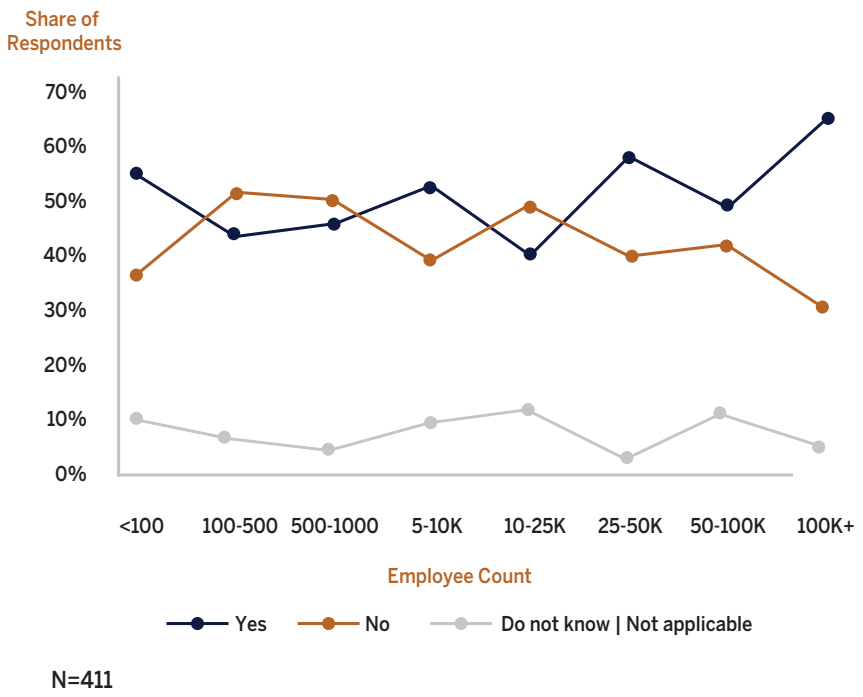
Three respondents brought up adding initiatives aimed at promoting the welfare and loyalty of principals' personal staff, as these team members can inadvertently create vulnerabilities. A common request voiced in the survey was to add people to the protection plan—specifically, additional tiers of corporate executives and broader coverage of principals' spouses, children, and other family members ("VIP family protection").

The Gap Between Threat Identification and Preparedness

How well do security leaders feel about their ability to face the challenges they identified? With regard to immediate physical threats, 70% of non-security firm respondents claim to have measures in place to combat top-of-mind threats, though only 46% of organizations believe they are doing all they can to mitigate them. When evaluated by size, only enterprises with more than 25,000 employees were consistently confident in their ability to manage the threats they identified as their biggest concerns.

Prepared to Address Top Threats by Organization

Q: Do you believe your organization is as prepared as it can be for the three threats you selected above?



N=411

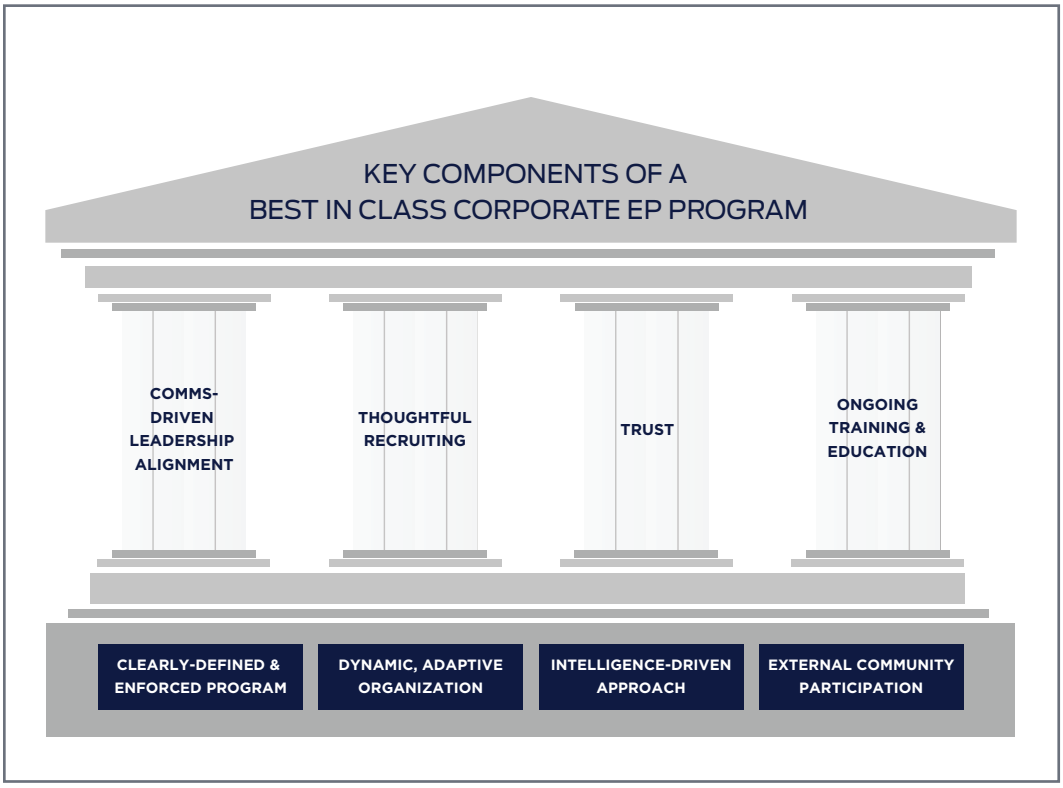
That a gap exists between the threats identified by executive protection teams and their ability to meet them successfully should come as no surprise, given the core challenges associated with delivering appropriate executive protection, as defined earlier in this report. No single prescription exists for overcoming this gap given the variability of organizations and needs. Instead, the journey to full preparedness must begin by identifying what "best in class" EP programs look like in order to extrapolate guidelines and recommendations that can be used to advance programs at all levels of maturity and sophistication.

Chapter 5

Exploring "Best in Class" Executive Protection

The question of defining best practices was—as one would expect—of great interest to research participants. Those representing more well-developed security programs had the most to say about best practice; participation declined with the self-described level of maturity. But as both the survey data and interview discussions reflect, best practice is less about specific tactics than it is about cultural mindset, awareness, clarity of mission, and organizational alignment.

Interestingly, the most common success factors revealed in the research are not dependent on high levels of resourcing, large organizations, or high risk profiles. They are equally applicable to all types of corporate protection programs and can be divided into two categories—the “foundational” components that underscore all successful EP organizations and the program “pillars” that can be built atop this strong foundation.



A CLEARLY-DEFINED AND ENFORCED END-TO-END PROGRAM

Respondents used a variety of terms to describe this: mission, standards, expectations, objectives, protocol, and response mechanisms. Two participants described it as a “scientific approach,” while another wrote, “a structured but flexible EP program under constant review for improvement opportunities.” Many also stressed the importance of disciplined adherence to standards that have been defined.

Advance work was a commonly picked-on example, as even seasoned professionals can fall into the “been there, done that” trap and fail to fully execute the advance plan. But beyond informing tactical preparedness, the benefits of having a clearly-defined methodology in place are clear: it enables consistent, comprehensive action based on a combination of strategic understanding and tactical preparedness, while further facilitating detached, dispassionate decision-making in the face of specific threats.

A DYNAMIC, ADAPTIVE ORGANIZATION THAT LEARNS FROM EXPERIENCE

The one caveat to the clearly articulated program vision described above is that such a program cannot be set in stone. The qualifying statement in the quote above describes this well: “under constant review for improvement opportunities.” Other interview participants noted an ability to “learn from mistakes (ours and others’)” and “always be asking questions” as being critical to proper EP practice. One went so far as to say, “open to new ideas and methods…not stuck in old ways,” and another called out soliciting executive feedback as a “best in class” practice.

Employing these types of active feedback mechanisms at the highest levels sets a cultural standard of dynamic problem solving rather than rote compliance, which is critical to effective programs given the constantly changing nature of various threats and risks. Both agents on the ground and program strategies must be able to, as one survey respondent put it, “plan for the worst, but be able to go with the flow as situations are fluid.”

Another aspect of this ability to evolve and adapt appropriately is to be able to do so in a systematic, fact-based manner. Every organization has its sacred cows, closely-held beliefs, and previously accepted standards. Regular, structured self-assessment and a culture that encourages the respectful challenging of long-held beliefs are important tools for helping those at the leading edge stay there.

Having protocols in place to scale and adapt as needed in the moment was another aspect of program definition that came up in discussions. According to Gavin de Becker & Associates, “we train and equip our Protectors to better handle inappropriate encounters and at a minimum they are required to have a bullet resistant vest, handcuffs, and a flashlight. Certainly other equipment can be added as the situation requires, but this is a company decision based on their training and the applicable Use of Force policies.”

Scale should also be considered in the broader sense; “best in class” organizations generally have well-defined plans and vetted resources on hand that enable them to scale up quickly when situations and/or travel to distant locations warrant it. One interviewee noted the advantage of not only knowing in advance who you would turn to in a moment of need, but of having them on retainer so that, “if an issue arises, you’ll be first in line for service.”

“’Best in class’ organizations generally have well-defined plans and vetted resources on hand that enable them to scale up quickly when situations and/or travel to distant locations warrant it.”

AN INTELLIGENCE-DRIVEN APPROACH

“No muscles, no guns,” was one of the most striking responses to the question of what makes a “best in class” program. A common refrain during interviews was the fact that executive protection is “more cerebral now” than it used to be, thanks to the growing prevalence of multifaceted intelligence operations.

EP has become a “smart” operation. “Best in class” teams monitor threats on multiple levels, with both static and dynamic information generated from sources both inside and outside the company. This provides insight at both a strategic and tactical level and helps aggregate information across risk categories—for example, cyber, political, brand/reputation, and geographic locations. Interviewees noted that bad actors tend to advertise what they plan to do; by simply paying attention a protection team can anticipate many, if not most, issues.

Many security teams begin this intelligence gathering process by monitoring open-source government advisories for high-level threat awareness at the most basic level. Travel assistance providers are often used to supplement this awareness with proprietary information in the form of more frequent updates and location-specific overviews of safety risks for travelers to a given area. Any number of third party subscriptions can provide snapshots of recent events or unfolding developments around the globe, with most adding their own predictions to summaries of events and implications.

While these static tools can help set expectations in advance, a comprehensive program will add sources of dynamic information as well. These may include, as some survey respondents noted, something as simple as Google Alerts or TweetDeck at one end of the spectrum, to sophisticated social media analytics software like Dataminr at the other. At the most granular level, this type of system can uncover and track breadcrumbs that may point to specific threats or provide valuable data around public sentiment. They usually also include internal system monitoring and issue detection tools linked to, for example, access control systems, email servers, or other mission-critical equipment. Depending on the space they are in and the resources that are available to them, organizations may go so far as to leverage deep web analytics or other proprietary government sources.

A third set of tools that come into play include those that help with trend and pattern analytics. From incident reporting software to proprietary analytics, capturing incident information and comparing it over time and geographies have become important capabilities. If a program is not keeping up with emerging threats and the sources to which they can be attributed, as one participant put it, “you’re flying blind.”

On the broader topic of technology, “intensive information gathering and intelligence programs,” as one survey respondent described them, are prompting greater integration of information and physical security efforts to enable the mapping of threats to assets’ locations. In some (usually larger) organizations, this integration has taken the form of security team restructuring to more tightly integrate information and physical security endeavors. In others, it has manifested in the emergence of fusion centers—collaborative efforts between two or more departments that share resources to facilitate stronger analysis—either alongside or as a function within the SOC.

Though fusion centers have historically been associated with the intelligence-gathering operations of local, state, and federal governmental agencies, their value is becoming increasingly apparent to private sector companies. Microsoft, for example, describes on its website that its Global Security Fusion Center, which is housed within its Virtual Security Operations Center in partnership with the company’s Global Security Communications Center, provides a “global information hub, monitoring emergent and developing world events around the clock.”[8]

CONSTANT, ONGOING TRAINING

Responses gathered from survey and interview participants suggest that “best in class” protection programs are “learning organizations,” in the sense that they “never stop training.” This commitment begins with specialized training; as Gavin de Becker & Associates noted, “a standard requirement of EP-specific training is needed and not just general police/military training and experience.” It is also ongoing. One interviewee shared that programs boasting annual trainings make him cringe; that the evolving nature of worldwide risk requires more than a once-a-year check-in. “Superior training” is how one survey respondent identified “best in class” from the rest; another noted that they outsourced their EP function entirely, because “we aren’t in the business of training.”

Participants cited the need for continual education of not only the security practitioners, but also of the principals they protect—and the organization at large—to create buy-in and “a security mindset across all aspects of the business.” One participant even noted that his organization included its security approach on the first page of the company’s onboarding materials. Another described seeing questions asked during quiet moments on car trips as opportunities to educate principals on their terms.

This education does not need to be formal, but it does need to be broad. As mentioned specifically in the earlier section, multiple survey respondents called out security training for executives’ families, and household staff as a best practice, because although the organization will set up controls and compliance to reduce risks from the inside-out, protecting them from the outside-in requires a behavioral focus. Principals and those around them must know and exercise their own risk-mitigating behaviors.

THOUGHTFUL RECRUITMENT

Manpower and human resources came up regularly in discussions of best practice. But more than simply having enough warm bodies, “best in class” organizations focus on finding quality talent and then maintaining it through training and culture.

Experience, unsurprisingly, topped the list of criteria security leaders look for when recruiting; for instance, they describe high caliber people as having global experience, being “well trained,” and having specialized skills. “Legitimate backgrounds,” according to survey and interview participants, may include relevant military or law enforcement service, governmental protection agencies like the U.S. Secret Service or Marshals Service, or the UK’s SIA certification program. Many also recognized third party credentials; those offered by Vehicle Dynamics Institute (VDI), Executive Security Institute (ESI), and ASIS International were mentioned specifically by survey respondents.

But many survey and interview participants also noted the benefits of hiring outside traditional backgrounds and feeder programs.

Multiple responses pointed to diversity of thought and experience as an advantage for any EP team; others pointed to “a strong academic background,” and people who “know how to think” as top requirements. More specifically, several participants referenced increasing reliance on technology and intelligence tools as a growing influence on hiring decisions. Information and analytics tools alone are not enough to run a high-performance security program; it takes human intelligence to turn the data they produce into actionable insight. As the practice of executive protection becomes more intelligence-driven, the skills needed are changing, which has opened the door to smart, analytical candidates from a variety of fields.

Regardless, interviewees stressed the importance of drilling down to understand the specifics of a prospect’s experience. According to one practitioner, “it takes more than one interview.” Resilience came up frequently as well. One interviewee noted that the most important thing he looked for in a candidate was the ability to de-escalate; that prevention is the whole point. “Ninety percent of issues can be resolved with a handshake and a smile.” Commented another participant, “You want a guy who sees going to hands as a failure.”

Similarly, “people skills” or “soft skills” have also become a high priority as EP teams expand. One participant pointed to the importance of character, work ethic, and team spirit. Professionalism was a key point of discussion as well. “You’re on display,” commented another, noting that personal appearance is important. A great agent will “walk authoritatively, be thankful and appreciative, and shake a lot of hands,” because doing so can help their principal get the access he or she needs.

Though the concept of soft skills was a popular one, more than a few participants went so far as to call out the fundamental need for a service mindset. One clarified that very few candidates have the right “disposition” for the work, as the requirements of corporate EP are “vastly different” than those of government or military assignments, given that executives often expect what one called an “armed, skilled concierge.” In reality, the responsibilities of protectors often involve mundane activities, such as picking up laundry or caring for a principal’s pet, and otherwise deflecting infringements on the principal’s productive time.

Those who are better equipped for success in the field recognize their role in thinking outside the box and anticipating “the small things.” In addition to required equipment, interviewees mentioned carrying personal ready kits, Band-Aids, Diet Cokes and water—even AEDs. One described carrying Shout Wipes, so that his executive would never have to face a press conference with a spot on his shirt. Candidates who feel themselves to be above this type of problem-solving, as multiple participants noted, will not be employed long. “Failure to prepare is preparation to fail,” as one respondent articulated. “It’s the small things that build your credibility and help them realize that you’re going to approach their safety with the same attention to detail. You have to give them faith.”

TRUST

Credibility is crucial to building trust, which may be one of the most basic cornerstones of a successful executive protection program. High-ranking principals can be demanding. They are known for making their preferences clear, and they do not often tolerate deviation from the expectations they have set—particularly in such close quarters. One director recounted that his principal had fired five previous protectors before he started, but that he ultimately won him over because the two were able to develop a professional respect for each other, as well as “a more human-to-human relationship.”

While the boundaries of the support relationship must of course be clear, protectors cannot “kowtow” to a principal. The most successful practitioners learn to understand them on a personal level. One interviewee described being able to speak frankly with the CEO he was charged with protecting. “Principals at this level are fact-driven. You have to give them the facts, but also give them solutions. They don’t want gray areas. You have to have the confidence to make it black and white for them.” Gavin de Becker & Associates stated that “The more professional the EP program, the more confidence the leadership has in their abilities. It is symbiotic.”

Building relationships and trust among adjacent departments and other stakeholders was also identified as a critical best practice. Participants mentioned the CFO, executive support staff, the IT department, and even the reception desk team as pivotal points of integration. As one participant put it, “there are a lot of cooks in this kitchen.” Without a unity of effort, constant communication, and trust among them, challenges can arise quickly. But when those stakeholders recognize the EP team as fair and responsible in their use of resources, asks of others, and appreciation of support—in other words, “we understand each other”—the protection process can be as invisible and seamless as it is intended to be.

Trust is an important part of third party vendor relations as well. Multiple participants commented that they require referrals or introductions from people with recent first-hand experience before considering a new partner. “This is the hardest part,” shared one Senior Director. Another described sending members of his team out to meet directly with potential third party vendors in order to confirm, face-to-face, that they were the right fit for their principals. “They have to be well vetted,” noted another, explaining that he needed to feel “as comfortable with those guys as I am with my own team.”

COMMUNICATION-DRIVEN LEADERSHIP ALIGNMENT

The importance of executive acceptance cannot be overstated. Protection simply does not happen without the support of organizational leadership and the buy-in of principals themselves. "It's all about the management commitment," commented one survey participant. Awareness and education are fundamental to this process, as are relationships. "You can't underestimate the role of relationships at the executive level," commented one EP leader. Having a champion among the C-suite team, and strong relationships at multiple levels of leadership throughout the organization, is critical not just for feedback and influence, but also to ensure that key messages are communicated.

In a world where program planning and new proposals can be difficult to get in front of busy decision-makers outside of an annual review period, having a network of supporters can help. When budgets are always tight, context is important. Being able to frame the impact of potential threats internally in a relevant and engaging way is critical to aligning necessary support. The VP at one enterprise described his job as being able to not just put a proposal together, but to "tell the story" around his requests. Another interviewee noted that selling the logistics benefits associated with solving safety challenges—such as saving time by never having to map a route or find a parking space—increased executive buy-in in conditions in which no clear and specific threats existed to prompt stronger security actions.

Ultimately, executive protection needs to be "a constant discussion." To use one survey respondent's words, it must be "an aggressive, open communication with the board of directors." The success of these discussions rests on a number of factors, not the least of which is a comprehensive, ever-evolving assessment of the threats at hand, backed up with hard data. It also helps for the security team (internal or outsourced) to have a strong understanding of the corporate environment and the organization's broader objectives so they can speak the same language and understand the trade-offs management may be considering.

At the same time, the EP leader needs to see him or herself as a full-fledged advisor to the company's leadership team—as the content expert on protection-related issues. "We are better as an industry when EP program managers see themselves as experts on security matters and certainly on all things EP related," noted Gavin de Becker & Associates. Just as the Chief Financial Officer or General Counsel view themselves as experts in their fields, "security should not be an exception." With confidence grounded in expertise, experience, strategic clarity, and knowledge of the greater environment, the executive protection leader can become a valuable contributor to the broader organizational leadership.

"In a world where program planning and new proposals can be difficult to get in front of busy decision-makers outside of an annual review period, having a network of supporters can help."

ACTIVE PARTICIPATION IN THE BROADER PROTECTION COMMUNITY

A number of survey respondents and interviewees also drew attention to the fact that the dialogue around executive protection must extend outside the company's four walls. One enterprise Security Director in particular commented that "best in class" companies "are active in OSAC, are always asking about best practices of other organizations, and are ready to collaborate with other organizations for best practices." Interviewees reiterated the value of groups like OSAC and ASIS, active alumni communities of (for example) Secret Service members, or local groups of EP professionals they met with regularly. However, they also noted that finding those opportunities can take some effort. As an industry cloaked in secrecy and with the highest standards of discretion and confidentiality, these forums are not always advertised openly.

The San Francisco Bay Area's tech community came up more than once as an example of a tight-knit group where many protectors know each other and where networking events are not uncommon, particularly after the recent YouTube office shooting. The financial services industry—banks, in particular—was referenced more often by survey respondents than any other industry as being "best in class" at executive protection; in part because of the high level of communication between its security teams. "It doesn't matter if they're competitors or not. They do a good job of getting together and talking about the issues they have in common." The "Three Lines of Defense," a risk management framework that gained steam after the 2008 financial crisis and has since been accepted as a best practice by the Basel Committee on Banking Supervision and federal banking regulators in many countries, has also likely encouraged this communication.

In its efforts to enhance banking organizations' self-governance, the model defines minimum standards and testing controls—including those of executive protection—for banks' risk management and compliance functions as part of the second line of defense. In addition to articulating universally accepted standards of care, the three lines of defense also sparked meaningful discussion and relationships among the banking community that, according to interview subjects, carry over to this day. While idea sharing across competitors seems unthinkable to many industries, "regular integration with peers to share knowledge and practices" appears to be a norm among banks with "best in class" EP functions.

"The dialogue around executive protection must extend outside the company's four walls."

Conclusion

In reviewing the results of this work, it is clear that the best practices of the world's strongest corporate EP teams are not that different from the tenets of "best in class" organizational leadership in general. In many cases, however, they diverge from the standards and practices prioritized within government and military executive protection, from which many security practitioners learned their trade.

For instance, executive protection within a corporation, as this research defines it, is risk-driven, but resource- and alignment-dependent. The balance (or imbalance) between these three factors sets the stage for how that program will be delivered. While executive protection has long been viewed as a "black and white," standards-driven field, the corporate environment brings with it shades of gray that can be difficult to understand and deliver against.

When executive protection professionals were asked to evaluate their programs, they tended to rate themselves modestly. At first glance, this could suggest that they are not performing on the level at which they should, or that they are struggling to command the resources and access they need. However, it may also illustrate that EP practitioners—particularly those with government and military backgrounds—may be tough judges who hold themselves to very high standards. Those standards may be more reflective of their prior career experience than their current organizations.

Regardless of how the situation is read, it suggests two opportunities. First, that corporate EP teams may benefit from greater customization of their program goals and standards to the specific realities of the broader organization in which they live, rather than adhering to a universal standard of care defined by practitioners operating under different circumstances. And second, that illustrating the rationale and intent behind these customized goals and objectives more clearly to the stakeholders involved in resourcing decisions—"telling the story"—may assist in remedying the lack of trust and buy-in many corporate EP teams experience.

Awareness of the unique nuances and dynamics at play in the world of corporate executive protection can always be improved upon, though this will not happen without concerted effort. In the spirit of keeping principals safe and enabling leaders to fulfill their missions, the intent of this report is to spur necessary dialogue about both the challenges at hand and how they can be best addressed. Communication and innovation remain the best weapons in our shared arsenal for staying ahead of adversaries; it is only by working together to push the collective thinking surrounding corporate EP that we will be successful in this ultimate pursuit.

Acknowledgments and Sources

Groundwork would like to extend our sincerest appreciation to several parties. First, to Gavin de Becker & Associates for their generosity in reviewing this analysis and offering their valued insight, as well as to ASIS International for their survey support. We are also grateful to all those who participated in the 2018 EP Practitioners Survey, and to those who volunteered their time and expertise through our supplementary interviews. We recognize and applaud your commitment to improving awareness of executive protection best practices through your contributions of your insight to this project.

In addition, we appreciate the following sources of information, cited as appropriate throughout the paper:

[1] GBTA, and Rockport Analytics. “GBTA BTI Outlook Annual Global Report & Forecast Prospects for Global Business Travel 2018-2022.” GBTA. Aug. 2018.

[2] Bobko, Vlad, et al. “2018 Risk Maps: Aon’s Guide to Political Risk, Terrorism & Political Violence.” Aon, 10 Apr. 2018, www.aon.com/2018-political-risk-terrorism-and-political-violence-maps/index.html.

[3] Grahf, Ron, and Ed Tyburski. "Employees Traveling Overseas: Managing the Risks of Unexpected Medical Emergencies." Zurich, 2011, hpd.zurichna.com/Whitepaper/Zurich-Employees-Traveling-Overseas.pdf.

[4] Gusovsky, Dina. "Companies Rush to Protect Against Kidnapping." CNBC, 10 July 2015, www.cnbc.com/2015/07/06/the-multi-million-dollar-business-of-ransom-.html.

[5] Barjon, Fritz. "Kidnap, Ransom, and Extortion Broker Playbook." AIG, 2017, www.aig.com/content/dam/aig/america-canada/us/documents/business/management-liability/aig-broker-guide-to-selling-kidnap-and-ransom-insurance-2017-final.pdf.

[6] Chan, Dr. Margaret. "Global Status Report on Road Safety." World Health Organization, 2015.

[7] Sleet, David A, et al. "Travelers' Health." CDC Yellow Book 2018, Centers for Disease Control and Prevention.

[8] "Global Security." Microsoft, 2018, www.microsoft.com/en-us/globalsecurity.

About Groundwork

Groundwork is the trusted provider of ground travel risk mitigation services, meeting the needs of power travelers who place a premium on time and convenience, as well as organizations that are serious about safety and security.

Groundwork offers protection services designed specifically for ground movements, while also delivering the personalized comfort and care of a bespoke traveler experience and the management ease and tools of an enterprise solution—across risk profiles, geographies, and preferences.

Our comprehensive managed ground solutions for executives and their security teams leverage three unique advantages:

- Full-time embedded secure ground specialists for onsite strategic advisory and logistical management of all your executives' ground needs.
- Fully integrated, proprietary mission management technology that enables GPS tracking, threat monitoring, real-time updates, and customized access to mission information.
- Our own dedicated team of Mobile Security Specialists, hand-selected and -trained local agents who execute every Groundwork mission around the globe

We specialize in one thing, and one thing only: secure ground movements. This clarity of focus helps us ensure that the same high standards are met consistently in every market, on every mission.

To learn more about Groundwork's services, reach out to the Groundwork team at 1.866.422.3535 (toll free) or +1.214.414.2425 (outside the US).

Inquiries: info@groundworkglobal.com

Press: media@groundworkglobal.com