Pearl Meyer

ARTICLE
| MAY 2026
| THE CORPORATE BOARD

Executive Security—From Perk To Necessity?

Sharon Podstupka

MANAGING DIRECTOR

Aalap Shah

MANAGING DIRECTOR

Originally published in the May/June 2026 edition of The Corporate Board, Vol. XLVII, No. 278. Reprinted with permission.

We are in an era of rising physical, digital, and reputational threats, and the security of executives can no longer be viewed as a discretionary perquisite outside the purview of boards' fiduciary responsibility. In its *2025 World Security Report*, security services firm Allied Universal found that 42 percent of security chiefs report a significant increase in violent statements against company executives compared to two years earlier. Furthermore, 97 percent of institutional investors say providing physical protection for executives of the companies in which they invest is important.

Executive security is now a material corporate risk that affects shareholder value and enterprise continuity. Are boards treating it with the level of rigor applied to other enterprise risks, and why should compensation committees care?

Compensation committees should care because executive security frequently intersects with executive pay oversight, perquisites, and proxy disclosure rules under US Securities and Exchange Commission Item 402 of Regulation S-K. When security measures are viewed as personal benefits rather than enterprise risk mitigation, committees may face judgment calls with regulatory, reputational, and say-on-pay implications. The concern is greater if security expenditures are perceived as executive benefits rather than risk mitigation.

One distinction is worth clarifying up front: Safety and security, while related, are not interchangeable. Safety programs are generally designed to mitigate accidental harm and ensure compliance with health, workplace, and environmental standards. Security, by contrast, addresses protection against intentional acts (including targeted physical, digital, and reputational harm). Investments in this realm have ramifications related to perquisite

disclosures.

To understand the implications of executive security, it is critical to first recognize how the threat landscape is evolving, and how it currently fits into overall board governance framework and enterprise risk management.

Pearl Meyer surveyed 258 companies across public, private, and not-for-profit sectors. The results point to a significant gap: Almost two-thirds (65 percent) of organizations lack a formal CEO security program, and only nine percent have adopted comprehensive, multi-layered security coverage.

> **A serious security incident involving senior leadership can disrupt operations, affect valuation, and erode investor confidence.**

These findings suggest that executive security has not, in many cases, been institutionalized within risk governance structures. As threat profiles evolve, formalizing oversight and aligning it with the board's broader risk assessment mandate can strengthen shareholder protection and enterprise resilience. This matters for two reasons:

- **Shareholders expect company leadership to deliver financial performance, but also expect continuity, stability, and protection of assets.**
- **Executive compensation should be viewed holistically, factoring in all elements "at work" (cash, equity, and benefits).**

A serious security incident involving senior leadership can disrupt operations, affect valuation, and erode investor confidence. Regardless of whether such an incident is a data security breach or a threat against a key executive, trust in the board's fiduciary responsibility to shareholders and investors may be compromised. However, the data indicate that executive security is treated as optional rather than essential from a board/governance perspective.

The risk environment for senior executives has changed in ways that boards should not ignore. Leadership decisions (including workforce reductions, facility closures, pricing actions, environmental strategies, or merger and acquisition activity) increasingly unfold in highly visible public and digital forums. Even when those decisions are strategically sound and aligned with long-term objectives, they can trigger intense public reaction.

In today's climate, that reaction may not remain confined to commentary or media coverage. Digital targeting, coordinated harassment, doxxing, and intimidation can extend into executives' personal lives, reaching their homes, families, and private digital accounts. The boundary between professional exposure and personal vulnerability has become increasingly porous.

Executives also face exposure during public appearances and travel, where widely accessible information and predictable schedules can increase vulnerability. Private air travel excluded, 44 percent of companies rank personal protection (e.g., secure ground

transport, bodyguards) as their highest-priority CEO security concern.

Cyber and physical risks are converging, but protections are not. According to the Pearl Meyer survey, cyber/digital protections rank among the top priorities (37 percent), reflecting growing attention to identity compromise, online tracking, and coordinated digital campaigns. By contrast, home security ranks much lower (eight percent), illustrating the challenge of aligning personal safeguards with expanding digital concerns.

Flexible work environments have become common in our more connected world, but assessment of risk has not kept pace. With evolving threat levels likely top of mind for executives as they consider competitive opportunities, it is increasingly important for compensation committees and boards to take notice. A thoughtful executive security framework not only serves risk mitigation, but becomes a recruiting and/or retention competitive advantage.

Despite the potential consequences, board engagement in executive security oversight remains limited. Considering the impact, this informality of oversight is notable.

The scope of executive security risks extends beyond the individual executive. For example, a targeted cyberattack against an executive's personal email or device offers a foothold into the corporate network. A physical threat or attack against senior leadership can disrupt decision-making, operational stability, and succession continuity. Even when no lasting harm occurs, such events can hurt shareholder value, as well as generate fear, distraction, and operational drag across the company, diverting management attention and affecting the "steady-state" stability most investors expect from corporations.

Despite these potential consequences, board engagement in executive security oversight remains limited. We found 58 percent have no formal role in security oversight, and only nine percent review or approve security policy and individual arrangements. Nearly 37 percent of boards never receive regular updates on security matters, and 46 percent are briefed only in response to an incident. Considering the impact that a serious security incident could produce, the relative informality of executive security oversight is notable.

While boards routinely establish accountability and reporting protocols for financial, cyber, compensation, and compliance risk, executive security is often seen as an operational matter rather than a governance priority. This lack of oversight results, in large part, from the view that executive security is a perquisite bestowed on a small segment of the corporate population, rather than a true exposure mitigation strategy. This notion is based in current SEC guidelines, and widely held across boardrooms and among the C-suite.

One of the more notable findings from our survey is the extent to which executive security decisions are guided by informal judgment (73 percent) rather than formal, structured

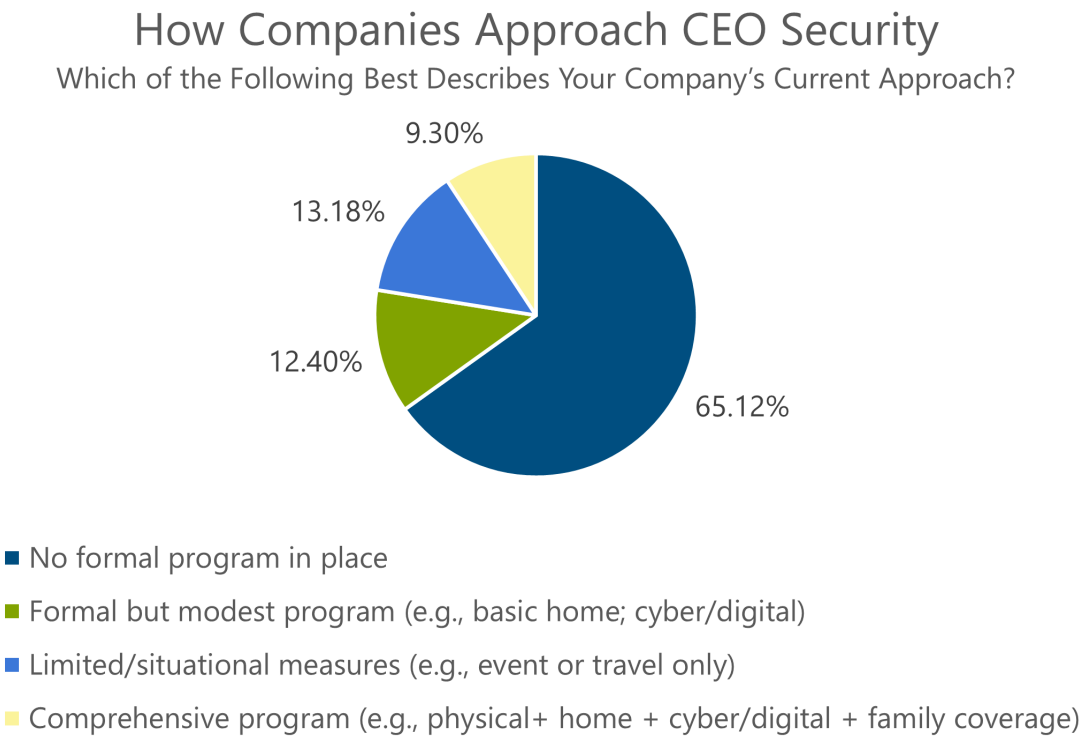
assessments (only 10 percent).

In other risk domains (e.g., financial reporting, regulatory compliance), boards typically rely on structured evaluation, data inputs, and defined governance controls. Executive security, by contrast, is often assessed without the same analytical rigor, despite its potential consequences. Threats on executives are not perceived to have enterprise-level impact.

However, the reality is that effective enterprise risk mitigation requires protecting your core assets. For many companies, people *are* the asset, and the way to protect that asset is multi-faceted: training and development, compensation, structured succession planning, and security.

> **Clarifying board-level oversight and integrating executive security into established risk frameworks helps ensure alignment with broader governance mandates.**

Without disciplined assessment, it is difficult to calibrate the scale, timing, or potential impact of threats facing executives, and the associated impact on enterprise and shareholder value. A more disciplined approach may include periodic independent safety analyses and monitoring of emerging geopolitical and sociopolitical trends. It should also incorporate intelligence on digital exposure threats, such as doxxing and social engineering; evaluate sector-specific issues; and gauge the visibility and vulnerability of executives in public, political, and social contexts.



Governance frameworks need to evolve to keep up with escalating vulnerabilities. This includes having the audit committee incorporate security reviews as part of risk assessment, and the compensation committee assess whether recommended security protections are a perquisite or an enterprise-level expense. Clarifying board-level oversight and integrating executive security into established risk frameworks can help ensure alignment with broader governance mandates.

Strengthening oversight does not require boards to manage security operations. Rather, it involves defining accountability, incorporating security into periodic risk assessments, reviewing policies and protocols, and engaging subject-matter experts as part of ongoing governance dialog.

Given the breadth of potential concerns, effective executive security programs should be wide-ranging. Yet our study indicates that only nine percent of companies have adopted comprehensive, multi-layered CEO security programs. These include physical protection, home security, cyber/digital defense, and family coverage. Another quarter take a limited approach, split between formal programs that only include basic home and cyber/digital protections (12 percent) and situational measures for specific events or travel (13 percent).

The data further highlight a lack of layered protection needed to address the full threat spectrum. Cyber/digital protection is the most frequently provided security measure (70 percent), reflecting the rapid rise of such risks facing executives and their families. Physical home security (54 percent), private air travel (53 percent), and personal protection services (46 percent) are in place, but trail cyber protection measures. Notably, private air travel appears in over half of programs, reinforcing its growing position as both a safety and efficiency tool rather than a discretionary perquisite. Only 11 percent of firms extend personal protection coverage to family members. While this indicates a logical focus on the executive, it potentially understates the vulnerability that a compromised family member can introduce.

Although more than half of companies provide physical home security coverage, this may not fully reflect the evolving exposure concerns in residential environments, which are increasingly viewed as less controlled than secured corporate facilities. Recent high-profile home invasions and security incidents involving prominent people have heightened awareness of residential vulnerability.

Market data reinforce this shift. According to a Christie's International Real Estate survey, 67 percent of US real estate agents report that security concerns are rising among affluent buyers (a group which includes corporate executives). Similarly, Coldwell Banker reports that about 45 percent of luxury homes sold in 2025 explicitly referenced privacy or security, up from 38 percent in 2024.

> **One constraint on executive security programs appears to be a governance dilemma—whether security should be treated as a business expense, or a perquisite.**

When security programs do not account for escalated safety concerns, companies encounter heightened disruption, increased crisis response demands, and reputational strain in the event of an incident. All of these can affect enterprise value. A coordinated approach that considers cyber safeguards, residential security, travel protocols, and family protections reduces the likelihood that isolated weaknesses become company-level events.

From a governance standpoint, integrating executive security into broader risk discussions can help ensure oversight reflects the full spectrum of exposure. Otherwise, security measures may not be consistently calibrated to the depth and breadth of evolving threats.

One constraint on executive security programs appears to be a governance dilemma—whether executive security should be treated as a business expense required for corporate risk management, or a perquisite that benefits members of the executive team. This distinction carries meaningful implications for SEC disclosure requirements, proxy statement language, tax treatment, and investor perceptions.

Pearl Meyer reviewed the proxy statements for the S&P 500 and found that 34 percent disclosed some sort of security perquisite, 78 percent of which involved aircraft usage. Of the remaining disclosures categorized as traditional security measures, the top two cited were personal protection (13 percent) and home security (10 percent).

The survey indicates that 42 percent of respondents classify most executive security expenses as business-related, consistent with the position that such measures are a company-driven necessity rather than an executive benefit. Nearly one-fifth (19 percent) disclose executive security as a perk, suggesting that some firms continue to take a conservative (or scrutiny-driven) interpretation of disclosure requirements.

Notably, 22 percent of respondents report uncertainty about classification, highlighting potential knowledge gaps between security operations, HR, and compensation governance.

This classification question carries practical significance as regulators, investors, and proxy advisors are increasingly scrutinizing executive security expenditures. Furthermore, SEC executive security disclosure practices are also receiving renewed attention. Under current SEC rules, security-related costs are reported as "All Other Compensation" pursuant to Item 402 of Regulation S-K.

During the SEC's June 2025 public roundtable on executive comp disclosure requirements, several industry participants noted that existing rules may not fully distinguish between discretionary perquisites and essential security measures. Some argued that treating essential security-related expenditures within the same category as personal benefits may create interpretive challenges and warrants reconsideration.

Despite the ongoing regulatory discussion, nearly 40 percent of respondents to our survey report no significant challenges in disclosing executive security costs in the proxy statement, and for the 24 percent that are not publicly traded, this is a nonissue. Approximately one-third indicate some level of complexity in disclosing executive security costs. The most common issue is distinguishing between business-driven security expenditures and personal benefit (14 percent), an area where evolving investor

expectations and regulatory requirements may complicate judgment.

> **On SEC disclosure requirements, boards may benefit from clarifying their governance approach to executive security.**

Other challenges include balancing disclosure detail and transparency with executive security concerns (eight percent), navigating taxation issues under IRS rules particularly on aircraft use (six percent), and providing sufficient rationale or context for investors and proxy advisors (three percent).

Although no timeline has been established for any revisions to SEC disclosure requirements, boards may benefit from clarifying their governance approach to executive security. This includes defining oversight responsibility, integrating security into enterprise risk assessments, and ensuring coordination among legal, HR, security, and compensation functions. Boards should also undertake comprehensive assessment of executive security needs, encompassing physical protection, cyber and digital exposure, residential security, and other relevant risks.

Compensation committees have a direct role because executive security expenditures frequently intersect with executive pay disclosure, perquisites, and proxy oversight under Item 402 of Regulation S-K. Committees can enhance their governance by requiring a documented, threat-informed rationale for recommended security protocols. Establish clear criteria for distinguishing corporate protections from personal benefits, and ensure proxy disclosure explains the business rationale for security measures in a manner investors can evaluate.

Given the limited scope of many programs and the current SEC disclosure rules, it is not surprising that reported investment levels are modest. Two-thirds (66 percent) of respondents indicate annual executive security spending (including personnel, equipment, cyber/digital, and travel) of less than $10,000. Only 10 percent spend $200,000 or more, a level more typically associated with integrated, multi-layered programs.

These lower spending levels are a function of the disclosure rules. The $10,000 threshold for disclosing executive perks, including executive security expenses, has been in force since the mid-2000s. It also suggests that many companies still view security as an occasional or transactional cost, rather than a sustained, year-round investment. Higher spending is not inherently indicative of effectiveness, but the distribution of investments suggests companies may be aligning expenses with disclosure rather than the breadth and complexity of the current threat landscape.

This is additionally notable given that only 39 percent of companies limit security coverage to the CEO. Among companies that extend coverage more broadly, protections may apply to select senior executives (32 percent), the full executive leadership team (22 percent), nonemployee directors (2 percent), or other groups (12 percent). Some report coverage

across multiple categories.

> **As companies expand executive security programs, shareholders are likely to seek clear articulation of rationale, scope, and cost.**

The mix of protections companies provide also reflects this tension. Cyber and digital safeguards are the most widely adopted (70 percent), likely because they align with existing IT infrastructure and enterprise risk frameworks. Traditional physical protection, home security, and family coverage are less prevalent, provided by 54 percent, 46 percent, and 11 percent of companies, respectively, and other unspecified protections account for 12 percent.

This distribution may reflect differences in how organizations categorize and justify expenditures. Cyber investments are more readily integrated into enterprise risk budgets, whereas personal physical protections may be evaluated through a pay or perk lens.

As companies expand executive security programs, shareholders are likely to seek clear articulation of rationale, scope, and cost, particularly where expenditures increase materially. Boards may also face increased pressure to clearly justify whether security measures are appropriately characterized as risk management expenses or compensation. Boards, and compensation committees in particular, will need to balance meaningful transparency with legitimate security considerations, providing sufficient context to support informed investor evaluation and satisfy governance expectations.

If security costs are disclosed as executive pay, they may influence investor assessment or proxy advisor analysis, particularly in sensitive pay environments. Because the compensation committee is responsible for overseeing executive pay disclosure, decisions about the classification, justification, and presentation of executive security expenditures fall squarely within its governance mandate.

For multinational companies, expanded programs can also introduce additional cross-border tax and reporting considerations that further heighten the need for structured oversight and planning. The survey findings suggest that executive security is evolving from an operational consideration into a governance discipline.

As that evolution unfolds, compensation committees are uniquely positioned at the intersection of risk, compensation, and disclosure transparency. Where security measures are necessary to protect leadership continuity and company value, committees must ensure that the rationale is documented, the classification is defensible, and the disclosure is clear and contextualized.

Executive security is not about optics or executive privilege. It is about preserving leadership capacity in a period when digital visibility, public scrutiny, and physical exposure increasingly intersect. For boards, the responsibility is to ensure that executive security is appropriately integrated into risk oversight and leadership continuity. For compensation committees, the question is not whether to manage security operations, but whether governance, classification, and disclosure reflect the risk realities facing senior leadership. In today's threat landscape, treating executive security with analytical rigor

and disclosure discipline is not ancillary to board oversight or compensation governance. It is an extension of both.

About the Authors

Sharon brings 25+ years guiding executive and broad-based pay communications and disclosure, helping boards and management manage change and respond to investor and proxy advisor scrutiny.

Aalap specializes in executive compensation strategy—governance, pay-for-performance, and incentives—helping companies align business, people, and compensation strategy for effective programs.

About Pearl Meyer

Pearl Meyer is the leading advisor to boards and senior management helping organizations build, develop, and reward great leadership teams that drive long-term success. Our strategy-driven compensation and leadership consulting services act as powerful catalysts for value creation and competitive advantage by addressing the critical links between people and outcomes. Our clients stand at the forefront of their industries and range from emerging high-growth, not-for-profit, and private organizations to the Fortune 500.