Pearl Meyer

ARTICLE | JUL 2025

Yes, CEO Security Prevalence is Increasing

Patrick Haggerty

MANAGING DIRECTOR

Mark Rosen

MANAGING DIRECTOR

The Backdrop: A Rising Tide of Executive Risk

CEOs are increasingly becoming targets of public backlash and political scrutiny. Risk factors ranging from physical safety to digital harassment are converging, and executive security policies that were once limited to high-profile companies and CEO founders are now expanding in prevalence and scale.

The tragic homicide of UnitedHealthcare's CEO in late 2024 is further accelerating the wider adoption of CEO security benefits that began in 2023.

What Data From S&P 500 Tells Us: Trends 2023 vs. 2024

Threats extending beyond the office and following executives into both personal environments require a blended strategy of physical and digital security. Recent proxy filings offer a rich set of data that reflect how S&P 500 companies are responding.

Our benchmarking captures 2023–2024 data across prevalence, cost, company size, and industry. It's important to note the following data do not reflect new or increased security measures taken in 2025 after (and presumably as a result of) the homicide of the UnitedHealthcare CEO. Anecdotally, in 2025 we have observed increased board

discussion around security, with many compensation committees implementing or increasing security for their executives. Such changes will generally be captured next year after 2025 proxies are filed.

Median CEO Security Prevalence and Cost by Type 2023 vs. 2024

The percentage of companies providing any type of CEO security increased from 28% to 34%. This marks a six percentage point gain and a 21% increase relative to last year.

Personal security grew in prevalence from 17% to 21%, while providing only home security was flat year-over-year at 11%, and providing only cyber security increased from 1% to 2%. It can be assumed that much of the cyber security protection for executives comes in the form of company-wide programs and processes. Note that some companies providing personal security also include home security and/or cyber security.

Median overall costs for all CEO security types decreased from $96,000 to $76,000 with new adopters often implementing more moderate programs and some companies feeling pressure to reduce costs overall.

2024 prevalence of security perk for CEO by type and cost by percentile

2024	Prevalence	25th %ile	50th %ile	75th %ile
Cyber security	2%	$4,000	$5,500	$5,750
Home security	11%	$6,387	$29,142	$184,130
Personal security	21%	$39,201	$103,529	$803,131
Overall	34%	$18,910	$76,032	$482,560

Personal security costs range significantly; the 25th percentile cost was almost $40,000 while the 75th percentile cost was over $800,000. CEO personal security programs typically scale with a leader's risk exposure and visibility. They often include protection personnel; residential and travel security; secure transport; cyber surveillance; and, in some cases, family coverage. The range in spend reflects varying risk profiles and program maturity—from targeted, risk-based protection to full-scale executive protection teams.

Understanding Adoption Profiles by Company Revenue and Industry

When segmenting S&P 500 companies into four equal groups by revenue size, we note that larger companies increased CEO security usage at higher rates compared to smaller companies. When proxies are filed in 2026, which will reflect actions taken in 2025, we expect to see a further increase in CEO security use across the S&P 500.

The largest group, companies with revenue at or above $28.5 billion, saw CEO security use increase from 50% of companies to 62% of companies, while the smallest group, companies with revenue below $6.5 billion, saw CEO security use increase from 10% of companies to 12% of companies.

2024 type of security perk by revenue size

2024	<$6.5B	$6.5B-$13.4B	$13.5B-$28.4B	>$28.5B
Cyber security	2%	2%	5%	1%
Home security	4%	10%	13%	16%
Personal security	6%	17%	16%	45%
Overall	11%	29%	34%	62%

Growth outside the largest companies suggests that more boards are evaluating exposure based on risk profile, though uptake among smaller companies remains comparatively limited. This disparity suggests smaller firms may lag in formal adoption despite similar exposure in some industries.

Independent of company size, communication services, financials, and healthcare sectors lead in personal security prevalence while real estate and materials industries lag.

Consumer staples and utilities showed the largest year-over-year growth.

Risk-based adoption is rising in sectors that traditionally have not offered formal protection, likely in response to social activism and public visibility. It remains to be seen which sectors may follow, particularly as public scrutiny and stakeholder engagement expand.

External Pressures Are Shaping Adoption and Cost Trends

Threat assessments are the driving force in the increased use of CEO security. More companies are formally referencing these threat assessments in their disclosures, with many companies concluding that the use of company aircraft for all business and personal travel, along with security services outside of working hours, is essential for their CEO.

At the same time, shareholder influence is placing pressure on cost. While prevalence increased overall, some companies took steps to cap costs in response to shareholder pressure following a failed say-on-pay vote. Glass Lewis has noted that “excessive” perquisites (including security related expenses) may serve as a harbinger for questionable practices, while Institutional Shareholder Services has issued “Against” votes where disclosure lacks transparency about perquisites potentially perceived as excessive.

An additional wrinkle is in the form of recent SEC dialogue questioning the treatment of perquisites. In June 2025, the SEC acknowledged in its executive compensation roundtable the need to re-examine how security expenses are defined and treated in CD&A disclosures. All of the panelists at the roundtable conceded that this was a delicate topic in light of recent events and were skeptical of whether security-related costs could legitimately be bucketed as a perquisite. It was noted the optics of including necessary and required security values in the perquisite category of the required tables distorts “total compensation” as a disclosure item.

Even when a company mandates security (whether or not the executive wants it), it ends up buried in the “Total” numbers. And this may be the only number that is analyzed by investors or proxy advisors. It appears that the commission may be open to revisit the definition of a perquisite (perhaps either excluding the value of security costs or providing for a higher threshold of security costs to trigger inclusion as a perquisite). It was also suggested that perhaps the value of security-related perquisites could remain in the proxy statement on a stand-alone basis but be removed from the Summary Compensation Table.

Aside from investor optics, there are legitimate concerns that required disclosure of the security measures have unintended consequences. While the disclosure provides investors with marginally more information, does it provide too much information about the exact protection that is provided to high-exposure individuals? Requiring less information could be more protective to those at risk.

A final pressure point is taxation of security perquisites which must also be assessed by compensation committees. This may provide a different and sometimes inconsistent

analysis from disclosure requirements. For example, under IRS rules, executive use of personal aircraft is generally considered a taxable fringe benefit unless it qualifies as a bona fide security concern, generally determined by an independent threat assessment or board-approved policy.

The Governance Imperative

From a governance standpoint, boards must ask whether security spending is justified by the risk posed, informed by third-party assessments, and properly disclosed and aligned with investor expectations.

Disclosure is a key factor. Poorly framed disclosure may lead to unwarranted scrutiny from proxy advisors and governance stakeholders and conversely, clear narratives can bolster trust and transparency. Proxies should clearly differentiate between necessary security-related costs and other perquisites to avoid misinterpretation.

Beyond an initial implementation of or increase in security, compensation committees can take a long-term approach to the issue by ensuring there is a defined, board-approved executive security policy. This can include defining whether it will be offered for similarly situated executives and/or offered to others on an ad hoc basis, and outlining how and how often threat assessments will be independently conducted. And as with other elements of executive pay, ensure costs are benchmarked and reviewed annually.

The executive protection landscape is evolving rapidly. Boards that take a proactive, measured, and transparent approach to CEO security, whether public or private, will be better positioned to protect not only their executives, but also their organization’s long-term reputation and the confidence of all relevant stakeholders.

About the Authors

Pat has 25+ years advising boards and senior management on incentive design, performance measurement, and corporate governance, with deep experience supporting both private and public companies.

Mark is a consulting team leader who brings 20+ years advising on executive and board pay, including benchmarking, retirement plan design, and tax/accounting and governance considerations.

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.