

Pearl Meyer

Quick Poll: Executive Security

Executive Summary

December 2025

Sharon Podstupka

Managing Director

sharon.podstupka@pearlmeyer.com

(202) 407 - 9551

Aalap Shah

Managing Director

aalap.shah@pearlmeyer.com

(347) 967 - 6442

Introduction

Boards today face a growing and often underestimated risk: the personal safety and security of their CEOs and executive teams. As physical, digital, and reputational threats accelerate, many organizations are making high-stakes decisions about executive protection without the structure, rigor, or governance these risks demand. Are current security programs sufficient? Are boards appropriately informed? And are companies balancing protection, transparency, and compliance in the right ways?

Pearl Meyer conducted a quick poll to understand how organizations are navigating this evolving landscape. The goal: evaluate the maturity of CEO security programs, examine where companies are investing across physical, home, cyber, and family protection, and assess how boards are engaged—if at all—in oversight and disclosure.

The bottom line is that most companies are behind the curve. Executive security practices have not kept pace with modern threat realities, and governance has not caught up with the decisions boards are increasingly expected to oversee. With clearer processes, more consistent assessments, and stronger board involvement, organizations can better protect their leaders while reducing risk and enhancing transparency.

If you have any questions or are interested in discussing these findings, please contact:

Sharon Podstupka, Managing Director
sharon.podstupka@pearlmeyer.com

Aalap Shah, Managing Director
aalap.shah@pearlmeyer.com



Survey Detail

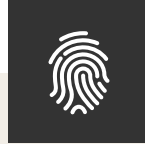
- + This survey was conducted in October and November 2025
- + 258 respondents from 125 public companies, 84 private companies, and 49 not-for-profit/government entities provided data

Key Highlights



Security Programs Lag Behind Modern Risks

- + Most companies still lack a formal CEO security program (65%).
- + Security posture is largely reactive, with 73% relying on informal judgment rather than structured threat assessments.
- + Majority spend under \$10K annually, signaling potential underinvestment relative to current risk exposure.



Cyber and Personal Protection Lead the Pack

- + Cyber/digital protection is the most common security feature (70%).
- + Personal physical safety is the top concern outside air travel (44%).
- + Home and family protections remain limited, suggesting gaps in comprehensive coverage.

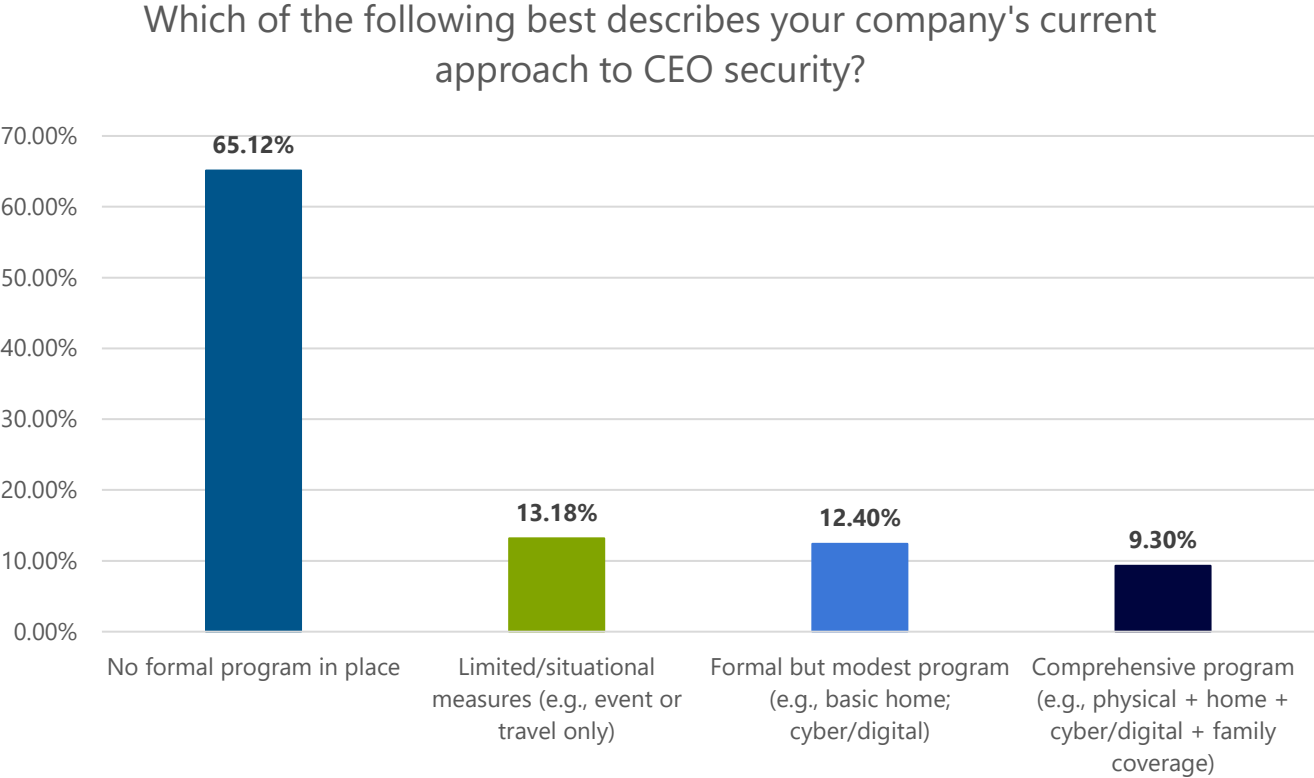


Governance and Oversight Remain Minimal

- + 58% of boards have no formal oversight role in executive security.
- + Nearly half receive updates only when issues arise; 37% never receive updates at all.
- + Mixed and inconsistent cost-treatment approaches highlight ongoing disclosure uncertainty.

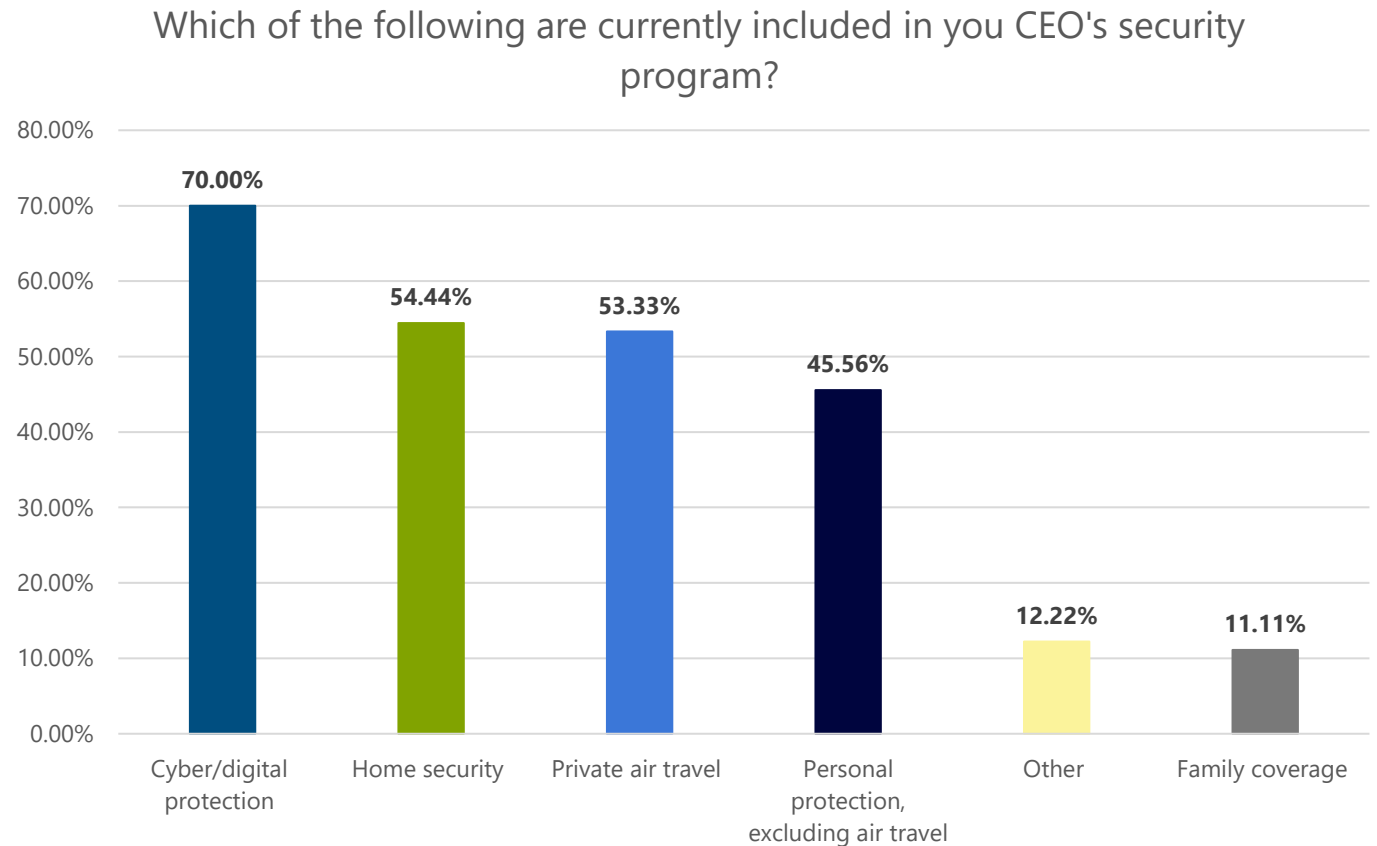
Which of the following best describes your company's current approach to CEO security?

- + Most companies (65%) operate without a formal CEO security program, underscoring how many organizations continue to view executive protection as discretionary rather than fundamental.
- + Only 9% have adopted comprehensive, multi-layered programs, demonstrating a small but emerging group of companies taking a more modern risk-management approach.
- + Approximately one-quarter of respondents fall somewhere between "none" and "limited," suggesting security needs for many companies are driven more by incident-based reaction than long-term planning.



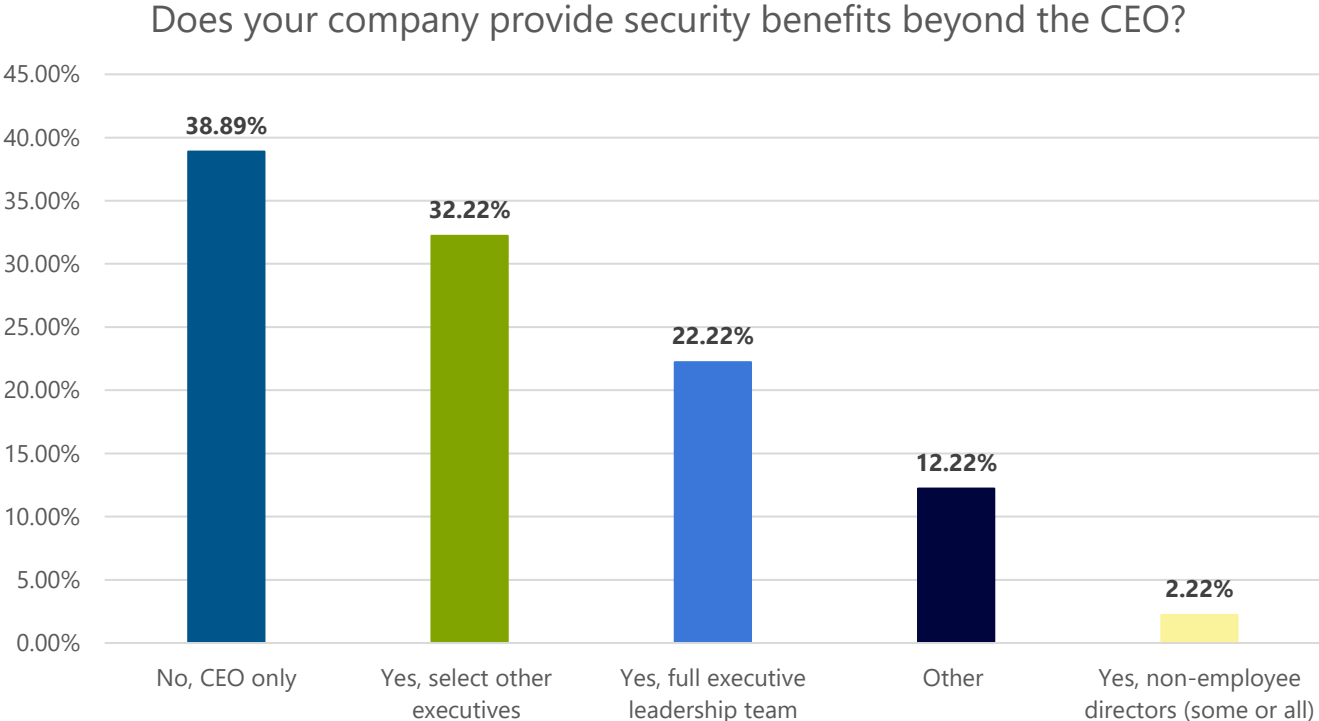
Which of the following are currently included in your CEO's security program?

- + Cyber/digital protection is the most frequently provided security measure (70%), reflecting the rapid rise of digital targeting, doxxing, and social-engineering risks facing executives and their families.
- + Majority of respondents indicate physical home and travel measures are in place but lag cyber protections, indicating many companies prioritize electronic risks over traditional physical vulnerabilities.
- + Private air travel appears in over half of programs, reinforcing its growing positioning as both a safety and efficiency tool rather than a discretionary perk.



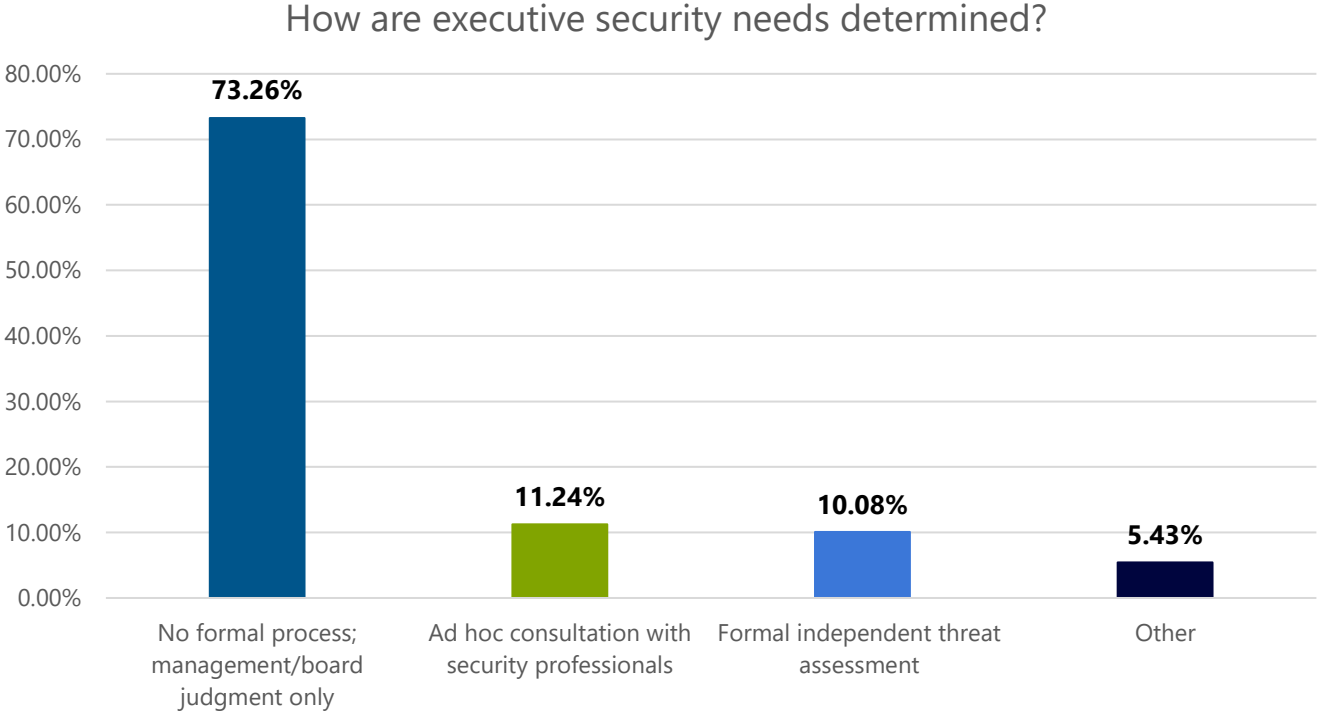
Does your company provide security benefits beyond the CEO?

- + Only 39% limit security benefits exclusively to the CEO, suggesting more organizations recognize broader risk exposure among other high-profile executives.
- + One-third extend protections to select C-suite roles, implying companies apply a targeted, risk-based rationale rather than hierarchical entitlement.
- + Extending security to directors remains rare, but its presence (2%) may hint at early signs of change as board visibility and cyber harassment increase.



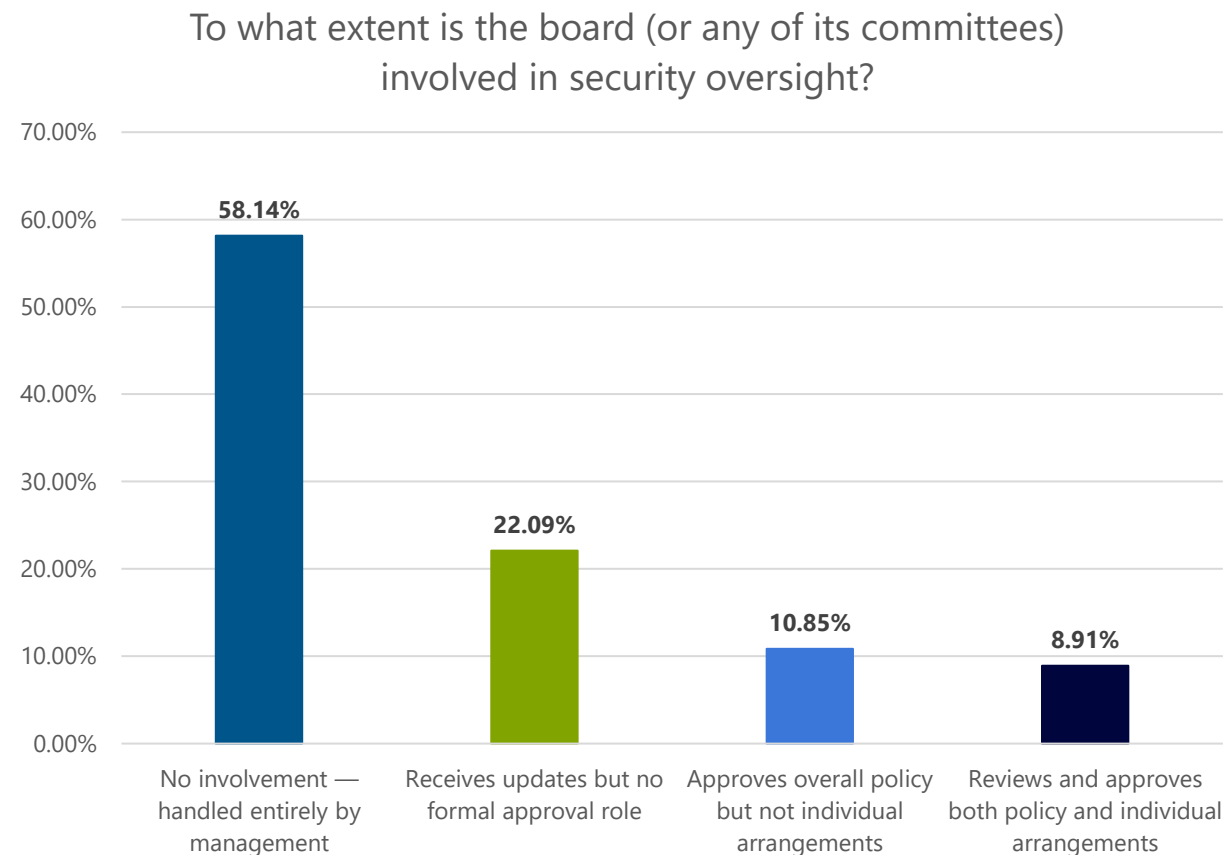
How are executive security needs determined?

- + The overwhelming reliance on informal judgment (73%) demonstrates that security decisions are still often made without structured input or independent threat validation.
- + Only 10% conduct formal threat assessments, indicating a missed opportunity to align security spend with documented risk levels and to strengthen disclosures.
- + The gap between perceived risk and formal evaluation suggests security policies may be outdated relative to the current threat landscape.



To what extent is the board (or any of its committees) involved in security oversight?

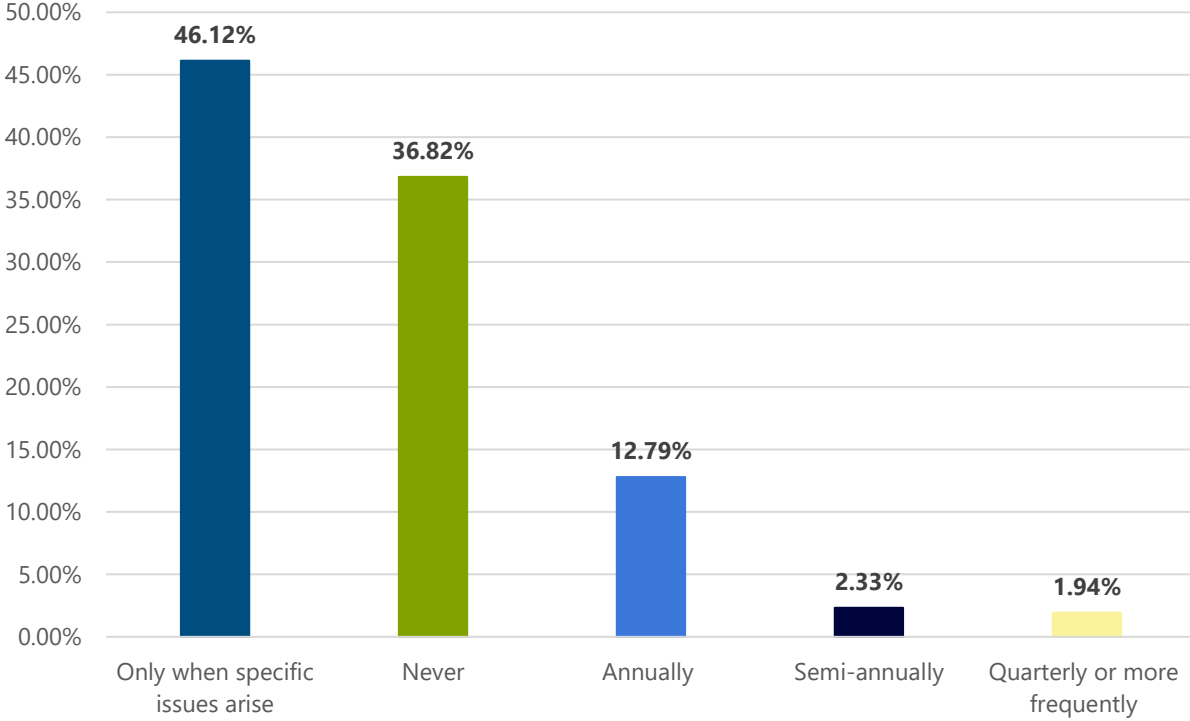
- + Most boards remain hands-off: 58% have no role in security oversight, despite growing scrutiny from shareholders and proxy advisors around CEO safety spend.
- + A growing cohort (roughly one-fourth) receives updates without approval authority, showing incremental progress toward transparency even if governance is still light.
- + Only 9% review and approve individual arrangements, positioning themselves as leaders in formalizing governance around executive protection.



How frequently does the board/committee receive updates on executive security?

- + Security is rarely a recurring agenda item: 37% of boards never receive updates, while nearly half only hear about issues when something goes wrong.
- + The low cadence suggests many organizations treat security as operational rather than as an element of risk governance—a potential point of vulnerability.
- + Almost 20% provides annual, semi-annual or quarterly reporting, signaling emerging best practice as threat environments evolve.

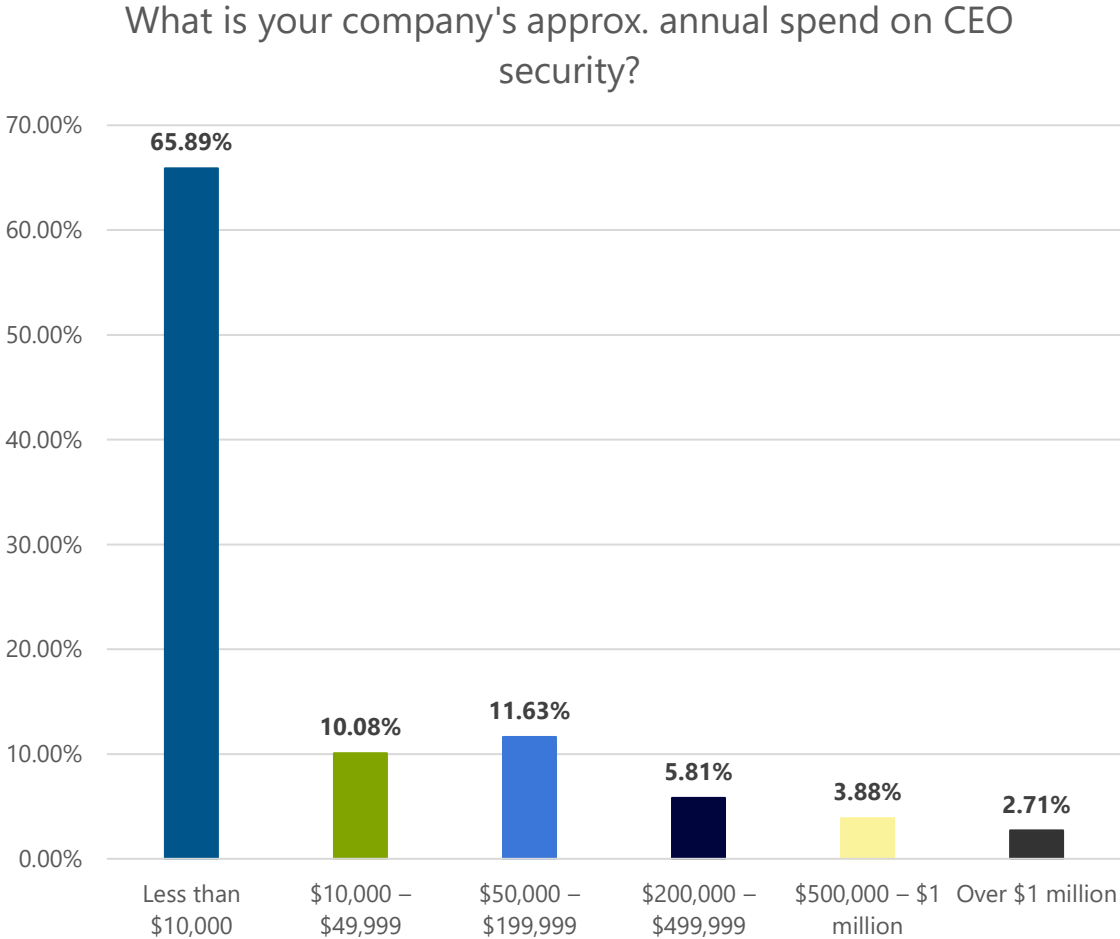
How frequently does the board/committee receive updates on executive security?



What is your company's approximate annual spend on CEO security?

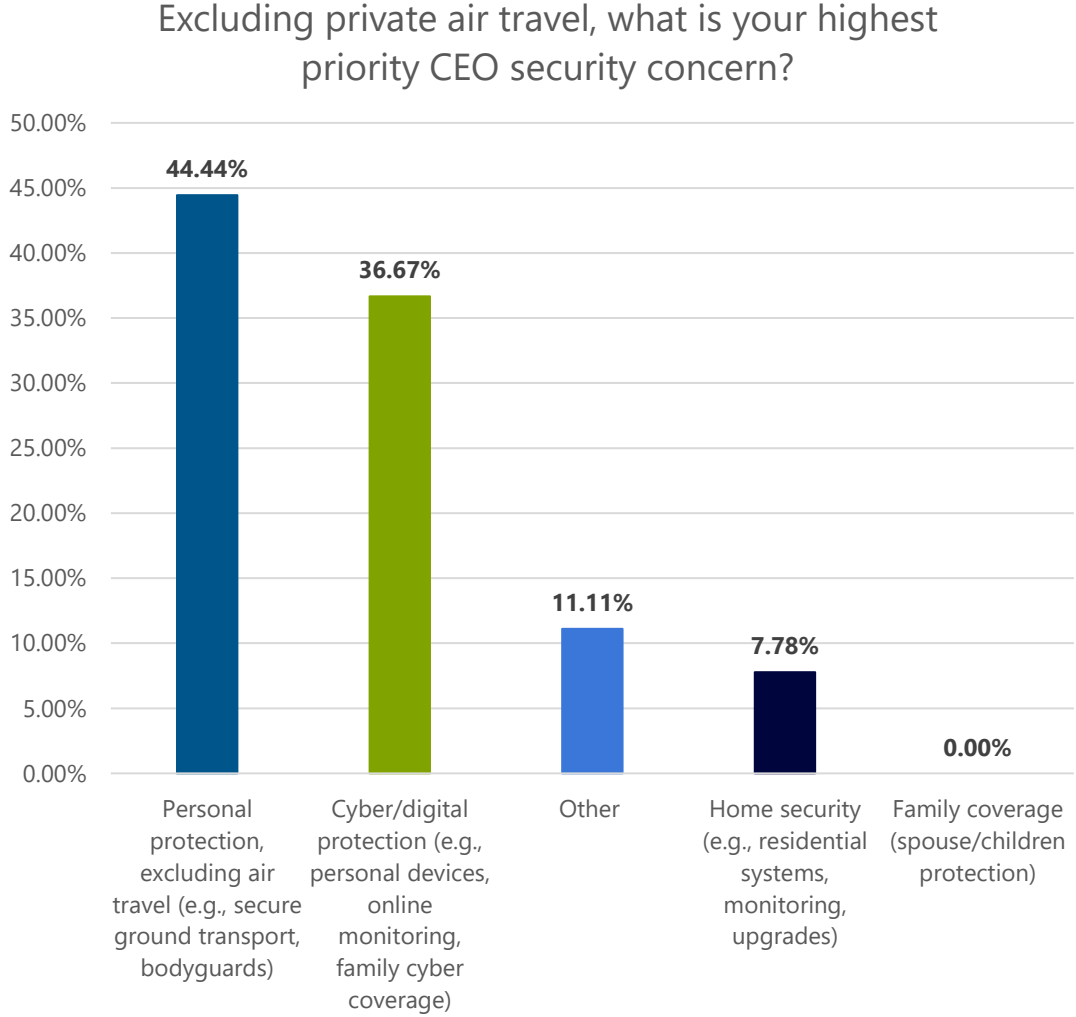
Including personnel, equipment, cyber/digital, and travel?

- + Two-thirds spend less than \$10,000 annually, indicating that many organizations may underinvest relative to actual executive exposure.
- + Only 10% spend \$200K or more, a level more consistent with fully integrated programs (physical, cyber, home, and travel).
- + The concentration of spend at the very low end reinforces that many companies treat security as an occasional cost rather than a comprehensive year-round program.



Excluding private air travel, what is your highest priority CEO security concern?

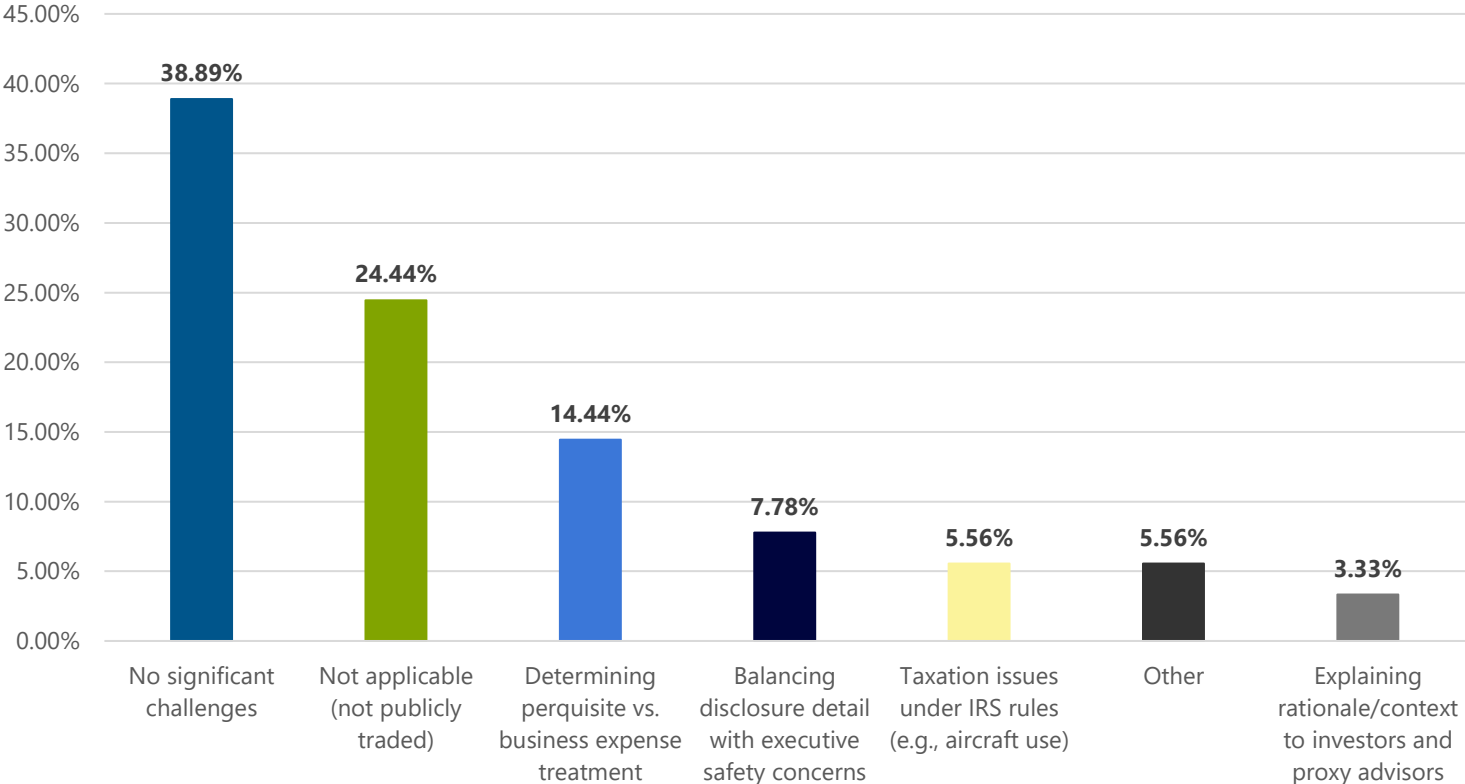
- + Personal physical safety remains the top concern (44%), highlighting persistent exposure during travel, commutes, and public appearances.
- + Cyber/digital threats (37%) are nearly as prominent, confirming that executives face growing levels of digital harassment, identity compromise, and online tracking.
- + Home security ranks surprisingly low, suggesting organizations may underestimate the convergence between digital threats and physical home vulnerabilities.



What is the greatest challenge for your company in disclosing executive security costs in the proxy/CD&A?

- + Nearly 40% report no significant challenges, suggesting companies with mature programs feel confident navigating SEC and IRS requirements.
- + For others, the predominant issue is distinguishing between business and personal benefit, an area where evolving investor expectations and regulatory requirements may complicate judgment.
- + Companies also struggle to balance transparency with safety, underscoring the sensitivities around publicly describing protective measures.
- + Tax treatment of aircraft-related security remains a recurring technical challenge.

What is the greatest challenge for your company in disclosing executive security costs in the proxy/CD&A?



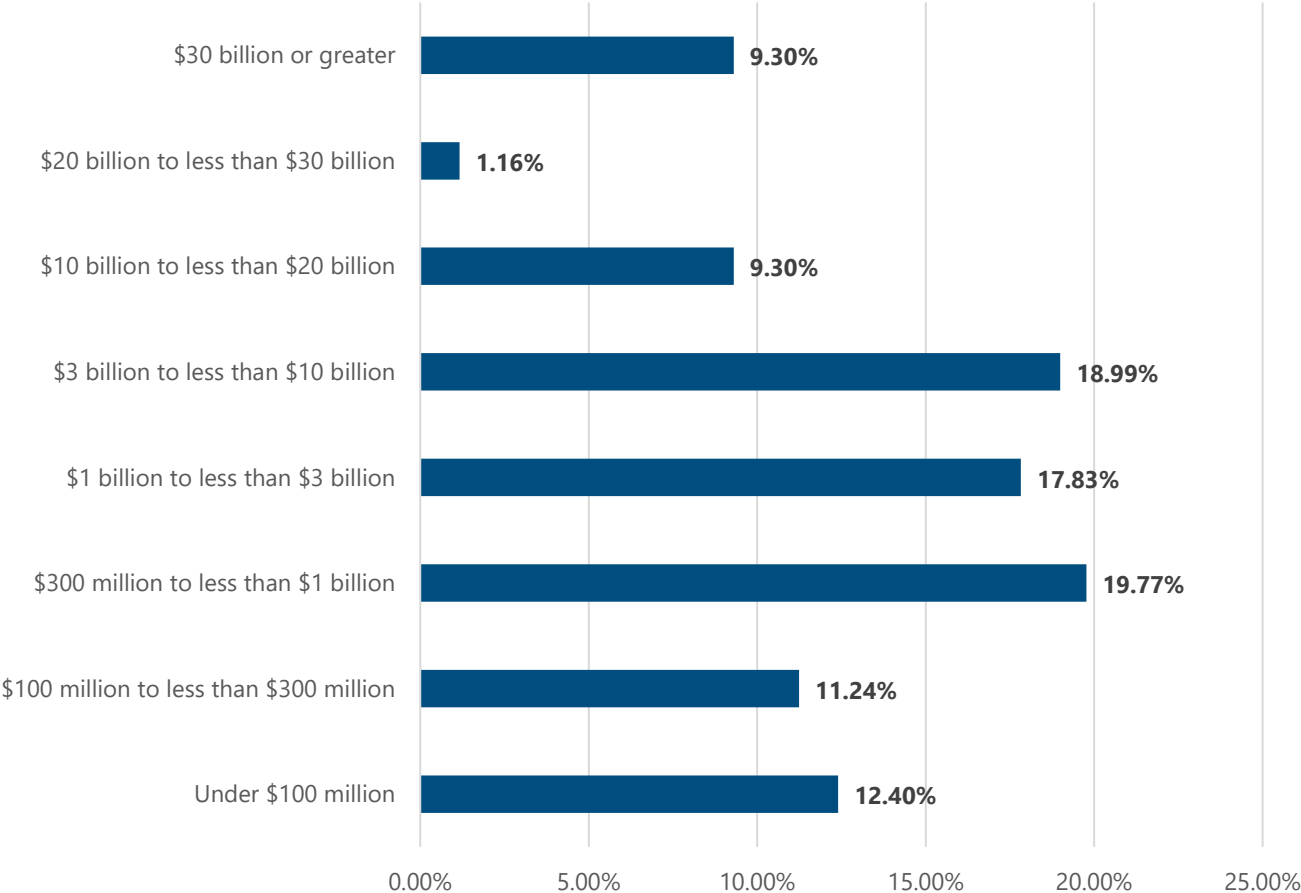
How are security costs treated for disclosure/accounting purposes?

- + The plurality (42%) classify most security expenses as business-related, consistent with the position that security is a company-driven necessity rather than an executive benefit.
- + Nearly 20% disclose security as a perquisite, signaling that some organizations continue to take a conservative (or scrutiny-driven) interpretation of disclosure requirements.
- + The meaningful share of respondents who are "not sure" highlights potential knowledge gaps between security operations, HR, and compensation governance.

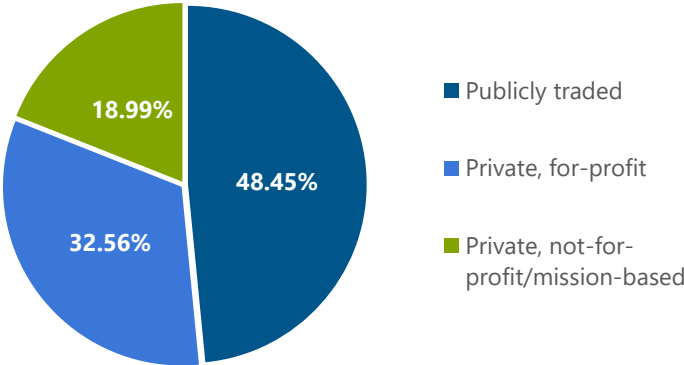


Survey Respondent Demographics

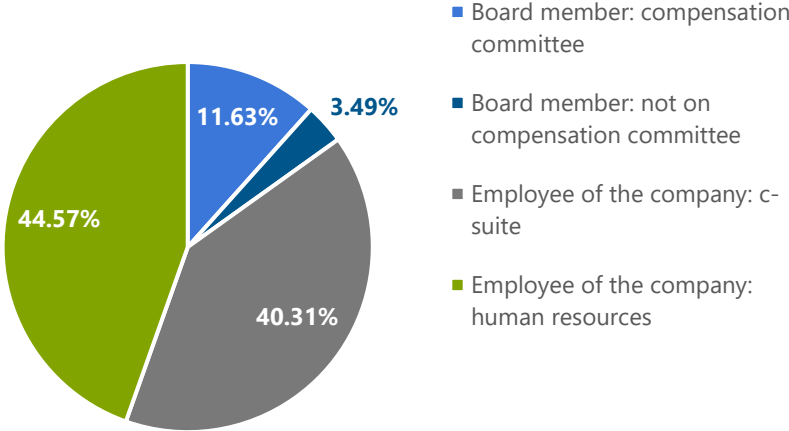
Revenue Range (or Asset Size)



Ownership Status

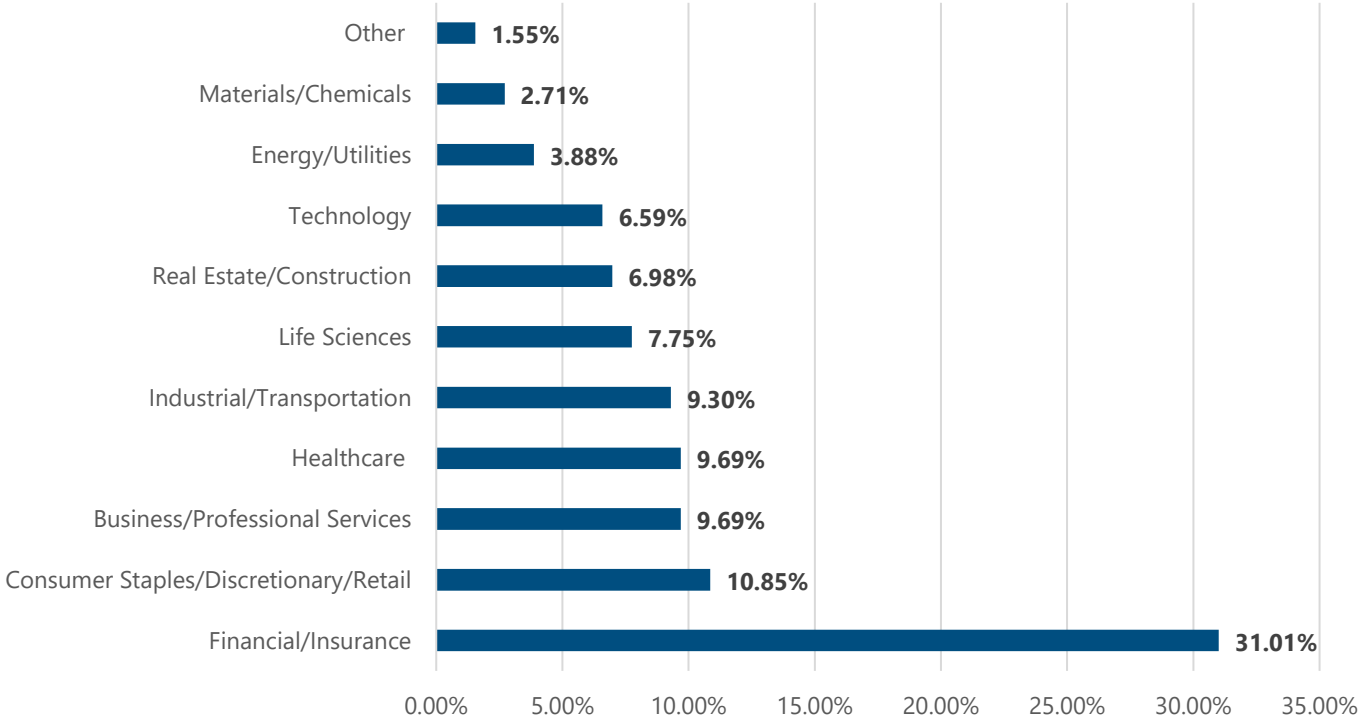


Respondent Role

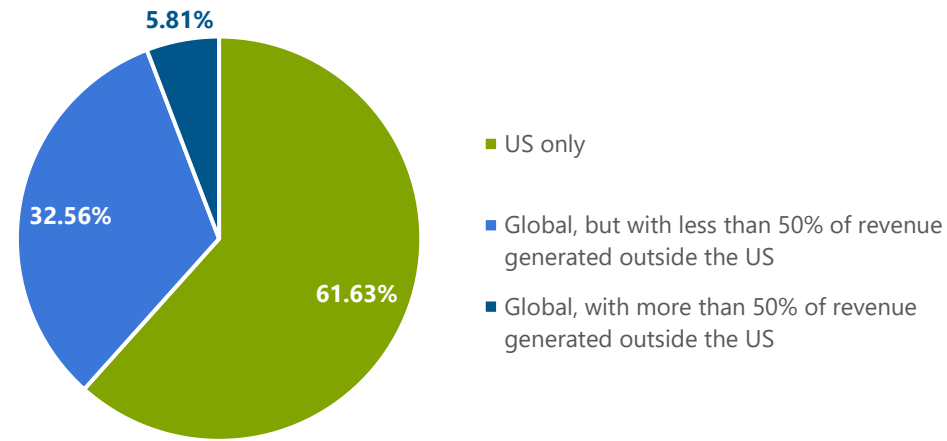


Survey Respondent Demographics (cont'd)

Industry

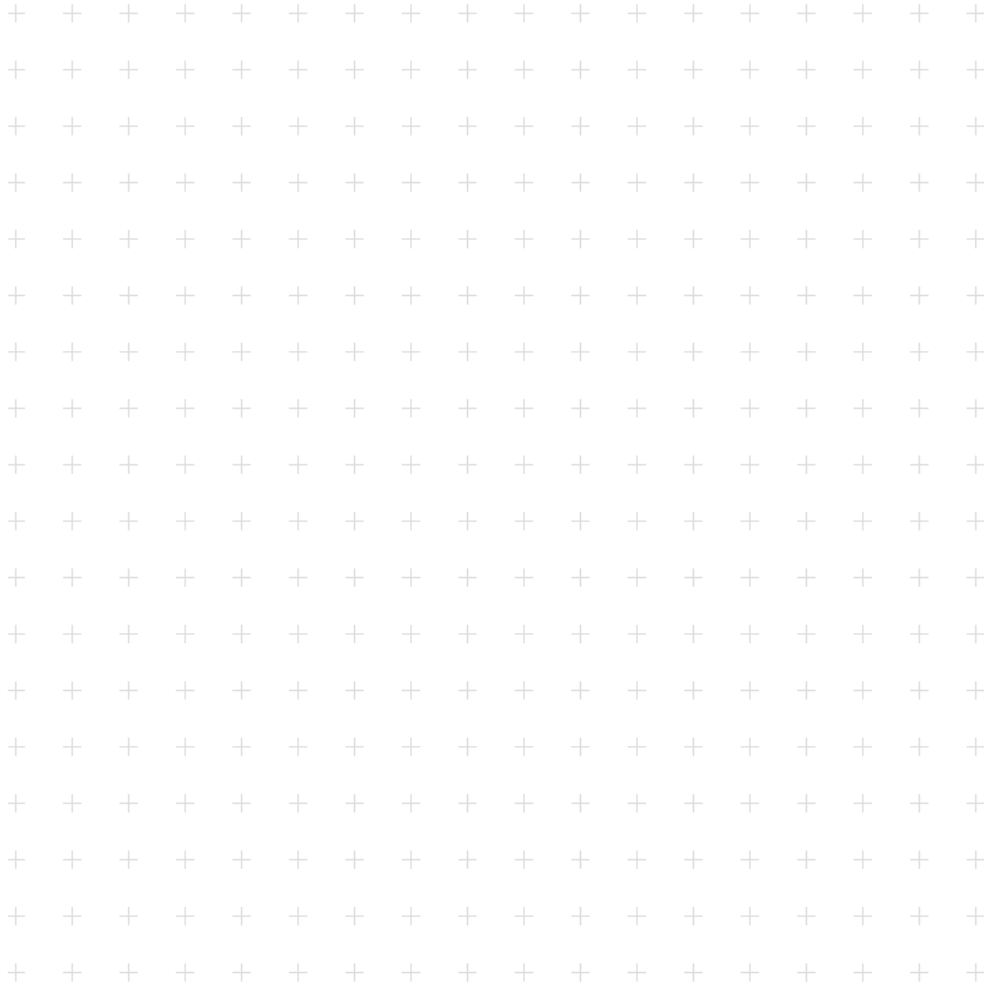


Geography



Pearl Meyer

Connecting People, Purpose & Performance



Thank You

For more information on Pearl Meyer,
visit us at www.pearlmeyer.com