



BY CHERYL STEELE

Vice President, Global Security & Resilience, Starbucks Coffee Company
Seattle, WA

THE EVOLVING ROLE OF CORPORATE SECURITY

In its “Future of Jobs Report” for 2025, the **World Economic Forum (WEF)** noted “Security Management Specialist” among its top five fastest growing jobs.

In its description, WEF cited “technology trends and geopolitical factors” as drivers behind the emergence of security specialists at the top of the list.

For many organizations, the responsibilities of security management specialists fall under the leadership of the Chief Security Officer (CSO). Traditionally, the CSO has overall responsibility, management, and leadership of:

- The physical protection of employees and corporate assets;
- Risk/threat assessment, mitigation and response; and (to varying degrees)
- Crisis preparedness, management and response.

The CSO’s remit may or may not include cybersecurity. In the WEF report, **cybersecurity** – “the art of protecting networks, devices and data from unauthorized access or criminal use and... ensuring confidentiality, integrity, and availability of information” – is captured as a distinct skillset and category from that of the CSO.

Future of Jobs Report 2025



Fastest growing and declining jobs by 2030

↑ Top fastest growing jobs

1	Big data specialists
2	FinTech engineers
3	AI and machine learning specialists
4	Software and applications developers
5	Security management specialists

↓ Top fastest declining jobs

1	Postal service clerks
2	Bank tellers and related clerks
3	Data entry clerks
4	Cashiers and ticket clerks
5	Administrative assistants and executive secretaries

The WEF report signals an evolving appreciation of the role and value the CSO can play in addressing a company's broader risk and preparedness posture. CSOs, the C-suite, and the Board have an opportunity to reframe what security managers can and should do in service of the organization.

Since the late 1980s, the acronym VUCA (Volatile, Uncertain, Complex, Ambiguous) has served as an organizing concept for leadership challenges in a changing world. Originally applied to the post-Cold War construct, VUCA is equally – if not more – relevant today. Organizations are facing a rapidly evolving risk landscape. These risks are wildly different today than they were even a year ago. Comfort and confidence in the face of a VUCA world is essential for any CSO.

This paper explores questions Boards should consider vis-à-vis corporate security and the broader risk landscape.

1

From “Gates-Guards-Guns” to... Business Enabler

When recruited for my first global security role several years ago, I was told, “we don’t need another subject matter expert in gates, guards and guns.” The “3-Gs” have historically been a convenient shorthand for the expectations of a CSO: the physical security and access control measures tied to the safety and security of people and places.

Delivering the 3-Gs is fundamental to the role of the CSO. Employee safety and security are often enterprise-level risks reported to the Board through the Audit and Compliance Committee. While necessary, delivering the 3-Gs is no longer sufficient.

In today’s multi-faceted and interconnected risk world, a CSO siloed in the 3-Gs is reactive. Far more effective is early engagement across the business and partnership in the broad landscape of enterprise risk. Cross-functional collaboration is key, particularly with those leading enterprise risk management. This critical collaboration enables forward-looking risk assessments and proactive development of mitigations and controls and allows a CSO to become an effective business enabler.

This pivot requires several areas of focus:

Championship at the top:

Does the C-Suite and Board see the CSO as a trusted partner in risk assessment and risk mitigation? Beyond ranking risks, does the enterprise routinely practice and test crisis response? Are risks thought of not in the vertical of a business unit, but in the horizontal and interconnected ways (operational, financial, reputational) in which they will likely occur?

Engagement in the P&L:

Is security a partner at the table when it comes to elements of business planning? Are elements of new market entry, site selection and site design considered through the lens of employee safety & security or business continuity? Is there space for security’s engagement in upstream strategy, or does it fall to downstream tactics?

Capability of the CSO:

Is the CSO equipped to partner with the business? Is the CSO oriented toward the engagement and outreach (a customer-centric mindset) necessary to build bridges within the organization? Does the CSO have a team with the skills to deliver on the core functional requirements as well as the thought-partnership and executive-level leadership demanded?



Defining a CSO's role in terms of both security and organizational resilience – the ability to prepare, respond to and recover from disruption and crisis – is a timely and important shift.

QUESTIONS FOR BOARDS TO CONSIDER

Does the board fully understand the organizational responsibility for employee and facility safety and security?

Has the company correctly assessed the degree to which employee and facility safety and security is a material risk to the organization across its entire footprint?

Is the company sufficiently weighing physical security risk in our broader conversations (i.e., brand reputation, new market expansion, mergers and acquisitions, etc.)?

2

UHG CEO Shooting and Managing through a Fluid Environment

The December 4th killing of a United Health Group CEO in New York City shone a bright light on the topic of executive protection. It prompted conversations among members of the Boards of Directors, C-Suites, CEOs, and security professionals. Many organizations found themselves asking, "Would we have been prepared? Are we prepared? Are we doing enough?"

Executive protection is the specialized skills associated with maintaining the personal security of high-profile leaders, such as the CEO. For many, executive protection is synonymous with the role of the US Secret Service in service to the President of the United States or of bodyguards supporting celebrities. In most companies, executive protection is part of a broader corporate security program and reporting to the CSO.

In the wake of any tragedy, there is an immediate focus on solving for that crisis. The attack of September 11, 2001 in the United States drove tremendous focus on airport and flight security. COVID drove an uptick in monitoring global health issues and a focus on supply chain risks. The United Health Care event in New York has driven a reexamination of how threats are monitored and how close executive protection is decided and deployed.

The public response to the assassination has also impacted security strategy and incident prevention. Rather than the expected shock and horror, there were instead instances of support and approbation. "Wanted posters" for CEOs appeared in New York's financial district. Voices of support and stories justifying/endorsing the violence appeared across social media channels. A "Deck of Cards" was created and marketed identifying a 52 "most wanted CEO" list.

Not surprisingly, this has driven an uptick in board of directors' examination of executive protection. Some have initiated third party evaluations or audits. At a minimum, the United Health Care attack has prompted fresh conversations between CSOs and CEOs on the scope of existing executive protection measures.

Executive protection is often thought of as the "close body person" – that individual (or individuals) near the principal, scanning the physical environment for any sign of imminent threat or risk. While a critical component, this approach is only one facet of a comprehensive executive protection program. Most mature programs are anchored by always-on threat monitoring: (1) chatter and conversation tied to the company and/or specific executives and (2) assessments of the physical location and environment of events and activities.



Assessments typically encompass social media channels – whether corporate-owned channels such as a company website or LinkedIn page, “earned” channels that reference the company or its executives, or other forums where discussion of an executive or a company may gain a share of voice or conversation. They also include other forms of communication, such as letters or emails. The goal of looking at communications and conversation is to assess whether there is an articulated or identifiable threat.

Assessments also focus on venue and format, specific to the vulnerabilities of a location (is it a public, open event; is it a private event with limited/managed attendance), etc.

Combining these two assessments enables executive protection programs to determine the level of risk a particular event presents and/or the level of support appropriate for the CEO or other executive.

It is important to understand executive protection as a two-way program built on mutual trust. It is a metaphorical handshake: on the one hand, the professional assessment and recommendations of the security team, on the other, the preferences of the CEO. It is a truly collaborative relationship. Some leaders may resist executive protection – perceiving it as invasive or overly personal. This is where trust, rapport, and candid conversation are critical:

Trust:

Does the CEO have confidence in the CSO and their executive protection program? Do CEOs understand how the security organization monitors and assesses risk? Do CEOs understand how risks will be escalated? Is there an understanding of what is and is not within the scope of the executive protection program?

Rapport:

Is there rapport between the CEO and the executive protection team? Do the style and approach of the executive protection team members mesh with that of the CEO and how the chief executive wants to be perceived/presented?

Candor:

The risks facing a CEO can be fluid as the headwinds against the company shift. The volume of the well-meaning concern of a CEO's close circle of family, friends and trusted advisors can vary. Does the trust and rapport of the CEO, CSO and executive protection team translate into candid and open conversations about the required scope of protection?

Executive protection is fluid. It is a dynamic interplay of (1) forward-looking risk assessment (venue, participants, visibility); (2) always-on risk sensing (new or lessening); and (3) differing stakeholder perceptions of the risk environment.

3

Evolving Risk Landscape: Doubling Down on VUCA

More than ever, security management demands an expansive and forward-looking view of the risk landscape. As the organization's leader for safety, security, and (often) resilience, a CSO is absorbed with how to effectively navigate the world of VUCA: Volatility, Uncertainty, Complexity, and Ambiguity and how to best navigate worst-case scenarios.

Three VUCA-loaded risk areas pose a specific challenge to the safety and security of people and places in today's world:

Geopolitics:

The world is deeply interconnected and increasingly fraught with tension. From reviewing the lessons learned from COVID-driven supply chain impacts, to navigating the forward-looking challenges of tariffs and trade policy. From disruptions to land, air, or sea transport driven by regional conflict, to evacuations or suspension of operations due to unrest or war. The complexity of geopolitical tensions has a clear and present impact on employee safety and the continuity of business operations. Events unfold quickly and can be hyper-localized (sites proximate to local protests) or regionally/globally dispersed (market exit or employee evacuations).

QUESTIONS FOR BOARDS TO CONSIDER

How effective is our organization in protecting executive managers?

Are we confident our security procedures are appropriate for a rapidly changing physical security environment?

Are we having the appropriate conversations with our CEO – both to reinforce the importance of executive protection in today's environment and to explore their confidence in the program which delivers it?



QUESTIONS FOR BOARDS TO CONSIDER

Brand reputation:

While historically thought of in terms of stakeholder impacts (employee, customer or shareholder), brand reputation can also manifest in physical security risk. The United Health case is perhaps the clearest and most startling example of how brand or industry perception can go from conversation to action with tragic consequences. A concerning trend is the sense of permissiveness for personal grievance to jump from complaint to action. Increasingly, organizations are expanding employee training to include formal de-escalation training. Many have also expanded to include disengagement training – knowing when and how to extricate and walk away from an encounter which is only becoming more heated. Thus, what starts as a brand reputation issue (poor customer experience), expands into a potential physical safety issue (verbal/physical conflict), which requires partnership with operations to address (employee guidelines and training).

Socio-politics:

We are seeing an increase in activation at the intersection of social issues and political dynamics. There is rising social polarization in many parts of the world, often driving civil unrest and upheaval. People everywhere are less likely to “talk” their way through disagreements or differences. Instead, they resort - almost from the start - to tactics that align more with anger and confrontation than persuasion. The more we see a tendency to “villainize” people, cultures or organizations, the more likely we are to see a sense of permissiveness for violent action.

1

Is consideration of the risk landscape sufficiently integrated into the physical security decisions corporate leadership is asked to evaluate?

2

Is the board confident that the business is adequately exploring knock-on (or “if-then... then what?”) impacts of key decisions through tabletop exercises or other means?

3

Does the organization know where it is physically vulnerable to changes in the socio-political landscape or geopolitical uncertainty – and are there plans prepared if the company needs to respond?

Conclusion

The role of the CSO has evolved. The urgency of the issues which a CSO can help an organization navigate have also evolved. While the core capabilities – or 3-Gs – are relevant as ever, CSOs today must excel in risk-sensing, risk-integration and risk-response/management. Today's resilient organizations must be equipped to leverage those skills.

I credit **Elisa Basnight** with developing a VUCA antidote that doubles as the defining competencies for future CSOs: vision to counter volatility, understanding to counter uncertainty, collaboration to address complexity, and agility to combat ambiguity.



ABOUT THE AUTHOR

CHERYL STEELE

Vice President, Global Security & Resilience,
Starbucks Coffee Company
Seattle, WA

Cheryl Steele serves as an Independent Director on the board of AlertMedia, a Vista Equity Partners (Foundation Fund)-backed company in Austin, TX. She provides voice-of-the customer insights for product roadmap and market strategy to this cloud-based provider of emergency communication and threat intelligence services. Cheryl is a regular presenter to the Starbucks Board of Directors, appearing annually in front of the Audit and Compliance Committee and the Employee, Partner and Community Impact Committee. She is an active member of the Board of the World Affairs Council – Seattle and previously served on the Board of the Freedoms Way National Heritage Area. Cheryl was also an elected member of the Town of Maynard (MA) Select Board, which provided executive management of the town, including budget and financial planning, union contract negotiations and community planning.

Cheryl is the Vice President of Global Security & Resilience at Starbucks Coffee Company, a global fortune 150 company operating more than 38,000 retail locations in 86 markets around the world. Cheryl's career spans executive and management roles across the private and public sectors. For Fleishman Hillard, she reinvented the Washington, DC office's business development lifecycle and led client capture efforts for several multi-million-dollar accounts. Cheryl directed Booz Allen Hamilton's work at the U.S. Department of State, the U.S. Agency for International Development, and special projects for the U.S. Special Operations community. At Booz Allen, she helped establish the Secretary of State's Office of Global Partnership Initiatives and launch the Global Counterterrorism Forum. She led strategic assessments of the Bureau of Foreign Assistance and managed international projects promoting accession to the World Trade Organization. Cheryl is a former diplomat at the U.S. Department of State with domestic and overseas assignments in the Middle East and multiple tours directly supporting the now head of the CIA, William J. Burns.

More about

CHERYL STEELE

Cheryl is an expert in integrated risk forecasting, planning and response.

She distills complex enterprise challenges into actionable programs, builds collaboration across business and functional units, and remains focused and deliberative during times of crisis or challenge. Cheryl is a strategic thought partner to the C-Suite, the Board of Directors and senior leaders across industry and sectors. A communicator, connector, and inspiring leader, Cheryl builds trusted relationships and has an established reputation for thoughtfulness, candor, and solutions-oriented thinking.

Cheryl is a lover of the outdoors who enjoys exploring the world; culinary adventures – whether cooking or dining; and local excursions with friends and family. She particularly enjoys opportunities to return to the Middle East, having lived in both Egypt and Jordan, where she can reignite her Arabic language skills. Cheryl earned her Master of Arts degree in Political Science from Columbia University in the City of New York and her Bachelor of Arts degree in Political Science and Economics from Hobart & William Smith Colleges.



Live Webinar

Strategic Impact Partners

Own The Future

Beyond the ESG Debate: The New Risk Management and Corporate Impact 2.0

Learn from these experts in this exclusive webinar.

Art Stewart
Managing Partner
Strategic Impact Partners

Cheryl Steele
VP Global Security & Resilience
Starbucks

Alethia Jackson
Senior VP ESG & Chief DEI Officer
Walgreens

Gary Robot-Moderator
Senior Advisor
Shared Assessments

📅 December 17, 2024

🕒 11:00 am - 12:00 pm EST

📍 Registration Required

🌐 BoardRiskCommittee.org

Watch the December Webinar with Cheryl Steele
Board Risk Committee Webinar: Beyond the ESG Debate:
The New Risk Management and Corporate Impact

UPCOMING EVENTS

BRC
BOARD RISK COMMITTEE

LEADING IN THE COTECH ERA


Why the Rules Have Changed

Wednesday, April 2
11:00am – 12:00pm EST

[RESERVE YOUR SPOT →](#) [BOARDRISKCOMMITTEE.ORG](https://boardriskcommittee.org)



YULY GROSMAN
Corporate Speaker



PATRICIA CHIN-SWEENEY
Executive Coach

[REGISTER HERE](#)

BRC
BOARD RISK COMMITTEE

[▶ WEBINAR](#)

DATA & DISPATCH

Intel and the Art of Negotiation in Cybersecurity

Tuesday, May 6, 2025, 11:00am – 12:00pm EST

SPEAKERS:
CAROLINE MCGLYNN
Global Head of IR Business Development,
Booz Allen

JENNIFER POLLIARD,
Director, Booz Allen

[RESERVE YOUR SPOT](#)
[BOARDRISKCOMMITTEE.ORG](https://boardriskcommittee.org)

[REGISTER HERE](#)

Who We Are

The Board Risk Committee (BRC) is a nonprofit, non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest.



SUSAN C. KEATING
BRC CEO



CATHERINE A. ALLEN
BRC FOUNDER AND CHAIR

CONTACT INFORMATION

Catherine A. Allen, Founder, Chairman, Board Risk Committee
cathy@boardriskcommittee.org

Susan C. Keating, CEO, Board Risk Committee
susan@boardriskcommittee.org

