FROM THE SOC TO THE BOARDROOM:
THE PATH TO FIDUCIARY READINESS

DR. EDWARD AMOROSO
Chief Executive Officer, TAG Infosphere | Research Professor, NYU | Former CISO, AT&T | Former Board Member, M&T Bank

INTRODUCTION

Every security practitioner will remember the first time they tried to make sense of security operations. They will no doubt recall viewing blinking dashboards, endless alerts, and a sense of how tough it is to achieve technical precision in processing security data. And for years, that was how the security operations task was performed with focus on hunting, patching, and remediating. While this was complex and difficult, it was certainly within the comfort zone of security experts.

Today, however, a growing number of CISOs who grew up with this operational mindset, are being forced to look past traditional security operations and confront a much different challenge entirely. This not some zero-day exploit, but a new expectation. Boards of directors now expect cybersecurity leaders to participate in **fiduciary governance,** not just operational defense. The journey from the SOC to the boardroom is therefore not a promotion. Rather, it's a **transformation** in mindset, language, and purpose.

Phase 1: Tactical Mastery

As we alluded to above, the first stage of most security careers involves establishing technical depth. It is where most of us learn to lead through competence. We earn credibility by understanding packet flow, by dissecting malware, by coordinating response during a midnight crisis. That mastery matters, and it's still an important pillar of trust. But it also forms a boundary. That is, technical mastery alone, however excellent, does not automatically translate **to fiduciary readiness.**

In the SOC, success is measured in indicators of compromise and time-to-contain. In the boardroom, success is measured in **trust and continuity.** The transition begins when a CISO starts asking a new set of questions. That is, thee CISO is on the right track when the question is not *"How fast can we respond?"* but rather *"What is the business impact of our resilience posture?"* Technical knowledge remains essential, but it becomes context, not currency.

Phase 2: Strategic Alignment

Once a security manager's technical base is solid, the next step is learning how the organization actually makes and reports money (even in government). I encourage every aspiring board-level CISO to sit with finance, risk, and legal teams. Study how your company measures value creation, how it discloses risk, how

it satisfies regulators. You'll discover that many cybersecurity objectives already align to these mechanisms. They just haven't been described in the board's language.

For example, instead of reporting "critical vulnerabilities reduced by 60 percent," translate that outcome into *"reduction of operational risk exposure by 60 percent within the enterprise risk appetite."* That subtle shift signals strategic maturity. It connects cybersecurity directly to the same taxonomy directors use for credit, market, and reputational risk. In TAG's interviews with seasoned board members, this fluency consistently ranks as the single strongest predictor of perceived executive readiness.

Phase 3: Financial Fluency

Nothing elevates credibility in the boardroom faster than financial literacy. Boards think in terms of **capital allocation** and **material exposure.** They want to understand how each dollar of security investment reduces potential loss or enables strategic resilience. A board-ready CISO should be able to articulate the following:

> **How a proposed SOC automation project improves EBITDA margin by reducing unplanned downtime.**
>
> **How the decision to purchase or retain cyber insurance affects risk transfer.**
>
> **How data protection programs preserve brand equity and intellectual property value.**

Answering these questions doesn't require becoming a CPA. It requires understanding that cybersecurity is a **capital stewardship function.** Directors respect a CISO who speaks the language of returns, trade-offs, and materiality because that is the language of fiduciary duty.

Phase 4: Governance Experience

The next developmental milestone involves increased exposure to **governance.** If you have never participated in a board or committee meeting, then speak with your boss about finding a way to do so, even as an observer.

Also, perhaps you can join an internal steering group, an external nonprofit board, or even the board of some industry consortium. You should use these opportunities to watch how agendas are structured, how minutes are crafted, how directors question executives. This is where many technical leaders experience their "aha" moment: realizing that boards don't decide how to fix things, but rather, they decide **how to oversee** them.

Governance fluency means understanding the core duties of directors and how cyber risk now intersects each one. When you can describe your security program in those fiduciary terms, you show that you belong in the conversation.

Phase 5: Presence and Influence

Like it or not, boardrooms test temperament as much as intellect. Directors look for confidence without arrogance, concision without evasion. You might have ten minutes to summarize the state of enterprise cyber risk, so every word matters. A high-Board-IQ CISO practices brevity. A good guide (obviously subject to specific guidance from your board secretary and boss) involves using three slides that show clear impact and a balanced tone.

Presence extends beyond the meeting itself. This includes how you communicate in public forums, interviews, or investor settings. The CISO who demonstrates calm authority under pressure embodies precisely what boards seek: a leader capable of protecting both systems and **shareholder confidence.**

Building Fiduciary Readiness

At TAG and Varonis, we define **fiduciary readiness** as the CISO's ability to participate credibly in governance decisions that affect enterprise value. It represents the culmination of four skill domains:

> **Strategic Context:** understanding how cyber aligns with enterprise risk and revenue.
>
> **Financial Acumen:** articulating return on resilience and cost-of-risk metrics.
>
> **Governance Literacy:** operating within board structures and oversight norms.
>
> **Composed Influence:** communicating with clarity and trust under scrutiny.

When these elements converge, the CISO evolves from a defender of systems to more of a **steward of integrity.** That's the inflection point where technical expertise transforms into fiduciary leadership.

From Defender to Director

Many CISOs I meet today also express a long-term ambition to serve on a corporate board. Buit this is not a simple process. Yes, boards do increasingly recognize that cybersecurity expertise is inseparable from enterprise risk oversight. But readiness requires more than tenure. It requires evidence of fiduciary mindset, and this is not easy for many CISOs.

Your résumé must read like that of a strategist, not an engineer. Your language must reflect governance, not configuration. And your demeanor must convey balance which is that quiet confidence that you can guide judgment under uncertainty. Those are the markers of fiduciary readiness.