SAMPLE QUESTIONS FROM A NOMINATING COMMITTEE

DR. EDWARD AMOROSO

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

INTRODUCTION

One of the most revealing moments in a CISO's career occurs not in a crisis call or an audit review, but across a polished table in front of a **nominating and governance committee.** The conversation lasts maybe an hour. No dashboards, no slide decks, no safety net, but just your judgment, composure, and the ability to explain what you believe about risk, leadership, and trust. Those sixty minutes determine whether a lifetime of technical expertise translates into **fiduciary credibility.**

Board interviews are unlike executive job interviews. The committee is not hiring you to run security; it's evaluating whether you can **govern** it. That distinction changes everything about how you prepare. Over the past decade, I've coached many CISOs through this process, and their success always hinges on the same principle: **Think like a director, speak like a steward, and answer like a fiduciary.**

Understanding the Committee's Mission

A nominating committee's mandate is to assess readiness for boardroom behavior, which includes independence, maturity, clarity, and cultural fit. Members will want to know that you can contribute to collective judgment without dominating the conversation or defaulting to technical jargon. They are asking themselves one question: *"Would we trust this person to help oversee the company's most sensitive risks in a calm, balanced way?"* Every inquiry they pose, no matter how tactical it sounds, ultimately tests that principle.

The Strategic Questions

You will almost certainly encounter questions, whether in front of the committee or with individual directors in a series of interviews (which is also common), that will probe how you link cybersecurity to **enterprise strategy.** Here are some typical examples:

> "How would you define our company's risk appetite, and where does cyber fit within it?"
>
> "What indicators tell you that a cyber investment creates shareholder value?"
>
> "How would you balance security improvements against competing business priorities?"

These questions are not pop quizzes on frameworks; they measure your ability to **think economically.** Directors want to hear how you weigh trade-offs, how you reconcile cost with resilience, and whether you understand that every control decision has financial consequence.

The strongest answers connect cyber posture to business outcomes: improved customer retention, smoother digital transformation, reduced regulatory exposure. Totally avoid defensive (but all-too-common) answers like "we must be 100 percent secure." The committee knows that's impossible. They want to hear risk tolerance expressed in language of *value protection*.

The Governance Questions

Next come the questions that explore your grasp of **fiduciary duty,** which is the legal and ethical foundation of board service. Here are some examples:

> "What does the duty of care mean to you in a cyber context?"
>
> "How would you handle a disagreement between management and the board about disclosure of a cyber event?"
>
> "Where do you draw the line between oversight and execution?"

These questions test whether you understand the difference between **governing and managing.** A high-Board-IQ CISO resists the urge to talk about tools or playbooks. Instead, explain how you would ensure that management has the right controls, policies, and reporting to meet the board's oversight obligations.

If pressed on a conflict scenario, emphasize integrity and process: "I would encourage transparency, consult counsel, and ensure the board fulfills its disclosure duty without compromising legal or operational integrity." That sentence alone signals you understand what it means to act as a fiduciary rather than a function head.

The Ethics and Culture Questions

Boards increasingly view cyber risk as a reflection of **corporate culture.** Expect questions that probe your values as much as your strategy:

> "How do you ensure security practices align with our company's ethics and values?"
>
> "Describe a moment when you faced an ethical dilemma in a security decision."
>
> "How would you approach disclosure of a material cyber event that might harm reputation but improve transparency?"

Your answers here reveal moral compass. Avoid platitudes about compliance; instead, describe **principled decision-making.** The best CISOs explain how they anchor choices in integrity and long-term trust, even when short-term optics suffer. Directors know that ethical courage, not technical brilliance, sustains reputational capital after a breach.

The Interpersonal Questions

Committees also evaluate **composure and chemistry.** They might ask:

> "How do you handle disagreement in the boardroom?"
>
> "What would your peers say about your leadership style?"
>
> "How do you simplify complex topics for non-technical audiences?"

These are behavioral signals. They're gauging whether you can collaborate without intimidation, speak plainly without condescension, and hold your ground without defensiveness. Practice short, sincere answers, stories that illustrate calm authority and humility. A board interview rewards presence, not performance.

How to Prepare

Think of preparation as three concentric circles: **content, delivery, and demeanor.**

> **Content –** Review the company's filings, strategy, and risk disclosures. Translate its mission into the language of resilience. Have a view on how cyber and AI intersect with its business model.
>
> **Delivery –** Rehearse concise, 90-second answers that tie security to governance. Practice replacing jargon with executive language: resilience, continuity, trust, materiality.
>
> **Demeanor –** Maintain composure. Pause before answering. Boards appreciate reflection over immediacy. Confidence lives in silence as much as in speech.

We often advise candidates to rehearse with a CFO or general counsel. They think in fiduciary terms and will quickly spot where your language drifts too operational.

What Not to Do

Do not bring slides or data. Do not mention tool names or vendor products. Do not describe yourself as "the technical expert." Boards already have experts. They need **governance experts** who can integrate technology into the enterprise's strategic conscience.

Also avoid overstating certainty. Directors value balance: "Based on our current threat intelligence, the risk appears moderate, but emerging AI models could change that profile." That kind of phrasing signals both mastery and humility, two traits directors prize equally.

Practicing Fiduciary Communication

Each question the committee asks is really an invitation: *Show us you understand the board's responsibility for trust.* Treat the conversation less like an interrogation and more like a rehearsal for future service. When you respond with brevity, composure, and strategic framing, you demonstrate that you belong in their circle of judgment.

As we often remind aspiring board candidates: the nominating committee is not looking for the best technologist in the building; they're looking for the calmest voice when the building is on fire. That, ultimately, is what distinguishes a board-ready CISO from a brilliant one who never leaves the SOC.

Final Reflection

The CISO community has matured from firewall management to fiduciary stewardship. The board interview is where that evolution becomes visible. Each question about risk appetite, ethics, or conflict resolution is a test of your **Board IQ** in action.

Prepare not to impress, but to reassure. Your job in that room is to give directors confidence that the enterprise's most complex digital risks can be understood, governed, and disclosed with integrity. When you achieve that, you are no longer auditioning for a seat. You are already thinking like one of them.