WHY HAVING A STRONG BOARD IQ MATTERS TO A CISO

DR. EDWARD AMOROSO

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

INTRODUCTION

For much of my career as a Chief Information Security Officer (CISO), the mark of a great security leader involved a high level of technical expertise. If, for example, you could explain encryption to a layperson, or recognize a malformed packet on a network, or lead an all-hands breach response, then you tended to earn the respect of the executive team – not to mention your own security team and peers. Technical mastery was indeed the currency of being a CISO for many years.

But that currency of security leadership has since changed. Today's enterprise risk environment demands a new form of literacy, one that transcends firewalls and frameworks. I call it **Board IQ:** an understanding of how boards of directors actually think, operate, and govern. And it is worth mentioning that this bleeds directly into an understanding of how your senior leadership team operates – including your CEO, CFO, and other non-security executives. Let's dig into this new responsibility.

From Systems to Stewardship

A CISO's technical knowledge once defined credibility. Now, it defines only baseline competence. The differentiator is whether you can translate security into **enterprise value,** and that means understanding governance. Board IQ is not about being more "executive-sounding." It's about seeing the company through the board's lens. This includes how directors weigh risk, assess management performance, and safeguard fiduciary duty on behalf of shareholders and customers.

When I ask CISOs preparing for their first board briefing what they believe boards do, the answers still surprise me. "Approve budgets." "Fund projects." "Set policies." All reasonable — and all wrong. Boards **do not manage.** They **govern.** That distinction sits at the center of Board IQ. Management executes. Boards oversee, question, and ensure accountability. They care about whether leadership is steering the enterprise prudently, not about which endpoint agent is installed on laptops.

What the Board Actually Cares About

A board's focus is narrow but deep: **strategy, oversight, and accountability.** It examines whether the business is being led ethically, competently, and in alignment with its declared risk appetite. Directors

listen for signals of resilience, such as whether the organization can absorb shocks without losing revenue continuity or brand trust. They care about governance posture, not configuration posture. In that context, the CISO's task is not to describe controls but to **connect them,** and to show how security decisions reinforce fiduciary confidence.

If you brief your board on ransomware, for example, then the question they're probably asking silently is **not** *"Which variant?"* but rather *"Could this event threaten continuity, compliance, or valuation?"* Similarly, if you were to propose an identity modernization initiative, perhaps during a board presentation, then they want to know how it mitigates regulatory exposure or reinforces executive accountability.

When you demonstrate that connection, you stop being a technical presenter and start being a **governance partner** – and this is obviously a good outcome.

Translating Cyber into Governance Language

Raising your Board IQ begins with vocabulary. Swap out operational verbs like *deploy, patch, and configure* for governance verbs like *oversee, align, and steward.* Replace acronyms with concepts. Use *resilience* instead of *incident response, enterprise exposure* instead of *attack surface,* and so on. This shift might feel semantic, but it signals a deeper realignment from control-center thinking to boardroom thinking. Do not take this lightly.

The metrics that you select and use should evolve as well. Directors respond to measures of **impact,** not activity. "Mean time to detect" may impress a SOC analyst, but a director would just hear a bunch of noise. Explaining something along the lines of "estimated revenue at risk under current controls" would get more attention – and yes, I know that is tough to estimate (even with models like FAIR).

The bottom line is this: Your board's ultimate mandate is to preserve trust capital, which is the belief among investors, regulators, and customers that the enterprise is being responsibly managed. Every chart and sentence in your presentation should reinforce that mandate.

WHY BOARD IQ DEFINES MODERN CISO SUCCESS

At both TAG and Varonis, our ongoing discussions with security leaders, reveal a pattern. That is, the CISOs who cultivate high Board IQ advance faster, influence strategy sooner, and gain broader portfolios of responsibility. They become, quite literally, **architects of resilience.** Their conversations with CEOs and directors shift from *"Here's what might go wrong"* to *"Here's how we sustain confidence when it does."*

We've also noticed (and perhaps this is not fully scientific, but the trend is clear) that these CISOs also earn greater budget latitude, because their framing justifies investment as risk optimization, not overhead. When a CISO can demonstrate that a $2 million automation initiative trims $10 million of potential exposure, then that CISO is now speaking the board's native dialect, which involves risk and financial consequence.

And one more thing: When the CISO's demeanor in the room shows composure under pressure, then that signals future readiness for greater management, leadership, and even governance roles for that CISO. Keep that in mind as you plan your own career.

The Human Element

Board IQ is not purely analytical. Rather, it's profoundly human. Boards are small ecosystems of personalities, including finance experts (common), former CEOs (also common), regulators, and even academics. They will test your calm, probe your logic, and sometimes challenge your confidence. A technically flawless answer delivered defensively will land worse than a composed acknowledgment followed by a thoughtful follow-up. Presence, not perfection, earns trust.

That trust, once earned (and it is not easy!), becomes the CISO's most valuable capital. With it, you can influence enterprise priorities, shape disclosure language, or advise on M&A risk. Without it, you remain a function head reporting upward, not a peer at the governance table.

From Defender to Steward

The evolution of the CISO, ironically, mirrors the maturation of cybersecurity itself from perimeter defense to **enterprise stewardship.** Just as security moved from IT silo to business enabler, the CISO must also now move from technologist to fiduciary partner. Building Board IQ is how that happens.

All of this really just starts small: You might begin by attending an audit-committee session. You should continue by reading (carefully) your company's entire proxy statement. You should learn (and observe) how your directors discuss material risk.

The goal is to develop the skills to translate your next security briefing into the language of shareholder value. Over time, you'll notice the dynamic change. The board will no longer view you as the person who "handles cyber." They'll view you as the person who helps ensure the company is **worthy of trust.**

The Defining Leadership Skill of Our Time

The purely technical CISO era is ending. Boards, regulators, and investors are aligning around a simple expectation: that cybersecurity be managed with the same discipline as finance, ethics, and operations. Meeting that expectation requires governance fluency, financial literacy, and executive composure, which are the pillars of Board IQ as we see it.

The next generation of security leaders will not be judged by the number of vulnerabilities closed or frameworks adopted, but by how well they guide the organization through ambiguity while preserving confidence. That is the essence of Board IQ and the defining security leadership skill of our time.