# DATA AS A BOARDROOM ASSET:
## WHY CISOS MUST REFRAME THE RISK NARRATIVE

**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 cybersecurity's history, data was treated almost like some sort of hazardous material, something to be contained, restricted, and defended against leakage. Entire programs, from DLP to encryption to zero trust, were built on the premise that data equals liability. That worldview is now obviously shifting, especially with artificial intelligence making **data is no longer merely an asset, but rather the capital** that drives business intelligence, processing, and decision-making. Yes — data is now a measurable source of enterprise value, much like cash, real estate, or intellectual property.

The implication for CISOs is quite profound. Elevating your **Board IQ** now requires understanding data not just as something to protect, but as something to manage, guide, and curate. The modern board now sees data as a form of currency that underpins growth, innovation, and trust. A breach doesn't just leak records, but rather, it erodes the company's credibility to manage its own capital responsibly. Let's examine this new role for data and how it affects and influences your work as a CISO and how you interact with your board.

### From Protection to Stewardship

The first mindset shift is subtle but transformative. Traditional security programs are organized around protection. Frameworks like NIST CSF 2.0 guide CISOs to focus on preventing theft, blocking exfiltration, and encrypting in transit. But when data is viewed as capital, the goal expands to **stewardship,** which involves ensuring that this capital is high-quality, well-governed, and responsibly used. This is not generally addressed in CISO training or in any of the frameworks used to guide CISO programs.

A steward doesn't just defend assets. Instead, they must ensure that those assets maintain (or appreciate in) value. For the CISO, that means framing initiatives like data discovery, lineage mapping, and privacy compliance as mechanisms of **capital integrity.** When you brief the board, avoid saying, "We're reducing data exposure." Instead, say, "We're enhancing the reliability of the company's data capital, ensuring it can be trusted for strategic decisions."

The fact is that in an era of AI boards can now instantly understand that language about data. Such focus can elevate cybersecurity from a defensive function to a governance discipline.

## Position Cyber Controls as Value Protection

Every control in your architecture, from access management to DLP, plays a role in protecting data value. When those controls work, they preserve the company's competitive advantage. When they fail, they devalue enterprise capital.

Consider intellectual property. A stolen product design isn't merely a confidentiality breach but should be viewed instead as a **capital loss event.** The same applies to customer data that drives analytics, personalization, and AI model performance. Framing your security controls as **value protection mechanisms** aligns security investment directly with the board's fiduciary priorities. This might seem awkward but making the effort to shift to this line of thinking will help you better connect with your leadership team and board.

Here's a practical example of what you might say: "Our DLP platform prevented the exfiltration of proprietary design documents, preserving approximately $15 million in potential intellectual property value." That kind of statement, which admittedly does not sound like something a traditional CISO would say, turns a technical function into an economic argument. It will resonate with directors because it quantifies how cybersecurity preserves shareholder equity.

## Quantify in Business Terms

The hallmark of a high Board IQ CISO also involves a reasonable level of fluency in **quantification.** The board's job is to weigh trade-offs such as risk versus reward and cost versus resilience. When you can meaningfully quantify cybersecurity in business terms, you make those trade-offs more visible. This should be comfortable with most CISOs because we've always been focused on metrics.

What we recommend is that you start to translate things like "records exposed" into concepts such as "financial exposure avoided." We need our teams – and yes, our vendors – to begin replacing "vulnerability remediation" with "risk reduction impact." We need everyone in the CISO ecosystem to begin anchoring their narratives in probabilities and outcomes. Here are a couple of good examples to help drive the point:

> **"This initiative decreases potential regulatory penalties by 40%."**
>
> **"This control preserves $8 million in recurring revenue by preventing data degradation."**

Numbers contextualize security in the language of governance. Even approximations, if well-reasoned, demonstrate maturity. Directors know uncertainty, but what they will value is if you can demonstrate a level of analytical thinking that is tied to enterprise consequence.

## Trust as the Multiplier

If data is the capital, then t**rust is the multiplier.** When customers believe you manage data responsibly, they will share more of it. This, in turn, drives innovation, personalization, and efficiency – especially for technologies such as AI. Trust compounds the value of data, whereas breaches can destroy it overnight.

CISOs must therefore position security as a **growth enabler,** not an inhibitor. A transparent, well-governed data program doesn't just avoid loss. Instead, it invites opportunity. When you describe your security architecture as the backbone of that trust, your executives and directors will start to see your function as strategic infrastructure.

## Build the Narrative of Responsible Data Capital

When briefing directors, weave a narrative around **responsible data capital management.** Start with the premise that data is a financial and reputational asset. Then show how your program safeguards its reliability, availability, and integrity. The goal should not be to avoid penalties, but to sustain growth.

Also – make sure to describe your work in the language of investment stewardship. This includes references to portfolio diversification (data segmentation), insurance (redundancy and encryption), and auditing (monitoring and assurance). Boards understand those analogies intuitively. Your goal is to guide them to see cybersecurity as corporate finance for digital assets.

# FROM RISK REPORTER TO VALUE PROTECTOR

The most effective CISOs I meet no longer identify as defenders of systems. They see themselves as **protectors of value.** They quantify exposure, demonstrate ROI, and express strategy in fiduciary terms. This is what separates a tactical security executive from a governance leader. In my own career, this was a difficult transition, but it was worth the effort – and I think the same will be true for you.

By reframing data as capital, you recast your mission from risk avoidance to **value preservation.** You also make it easier for directors to champion your initiatives because you've connected them directly to shareholder confidence. The conversation moves from "Why are we spending this much on DLP?" to "How can we strengthen our data capital position?"

## The Boardroom Mindset

As we have argued above, boards increasingly recognize that trust will define the winners and losers of the next decade. They will expect CISOs to articulate how their organizations collect, govern, and protect data as a matter of fiduciary responsibility. That's the new frontier of Board IQ – and you should take this seriously.

When you walk into that room and speak about data as capital with metrics, ethics, and stewardship intertwined, you signal that cybersecurity has matured into a core governance discipline. And when that happens, the CISO's seat at the board table becomes more indispensable.