# TEN THINGS CISOS SHOULD KNOW ABOUT PUBLIC BOARDS

**DR. EDWARD AMOROSO**

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

## INTRODUCTION

If there is one management topic that seems to unite Chief Information Security Officers (CISOs), it is their uniform agreement that communications and interactions with their company board can be both a strategic opportunity (if done right) and a daunting consequence (if done wrong). For this reason, guidance on how best to work with boards, especially in public companies, is important for CISOs – hence, this article.

As preface, we feel obliged to comment that CISOs will usually find a long chain of reviews and curations that occur from the time an idea is proposed for sharing with the board and the actual messaging delivered during a meeting. It is a fiction that CISOs will have full latitude to determine how to present to the board. This is a curated activity, so everything we suggest below is subject to that important component of the process.

In addition, we must acknowledge that every public board, even for companies that might seem comparable, can be fundamentally different. So, readers should therefore be careful to tailor any guidance below to their local context. That said, we can share some general traits regarding the culture, expectations, and operations of public boards. To that end, here are ten key insights, in no particular order, that we believe every CISO should internalize:

## TEN INSIGHTS FOR CISOS ON BOARDS

### 1. Boards Are Focused on Risk and Business Outcomes

Boards must prioritize enterprise risk, shareholder value, and long-term business resilience. CISOs must therefore connect cybersecurity risks to financial and operational consequences, framing security not as a technical issue, but as a business enabler or blocker.

### 2. Cybersecurity Is Now a Fiduciary Responsibility

Following regulatory pressures and incidents like SolarWinds, public boards are increasingly expected to oversee cybersecurity risk. CISOs should prepare to explain how their programs align with governance obligations and legal exposures.

### 3. Directors Speak in Financial Terms

Unlike CISOs, board members rarely use technical jargon. Effective CISOs translate security investments into metrics like return on investment (ROI), total cost of ownership (TCO), and impact on enterprise valuation.

### 4. Time Is Limited, Messaging Must Be Sharp

Board agendas are tightly packed. CISOs typically get 15 minutes, often annually or quarterly. Every slide, sentence, and data point must be curated for clarity, impact, and brevity.

### 5. Public Boards Are Politically Nuanced

Boards have power dynamics, alliances, and factions. CISOs should be politically aware, understand who champions cyber, and tailor communications accordingly to key directors.

### 6. Public Filings Increase Visibility

Public companies file 10-Ks, 8-Ks, and proxy statements, all of which may reference cybersecurity programs and incidents. CISOs must coordinate closely with legal and investor relations to ensure accuracy and consistency.

### 7. Independence and Transparency Are Critical

Boards value honesty and independent thinking. Sugar-coating incidents or hiding risks can backfire. CISOs should build trust by reporting truthfully and transparently.

### 8. Board Committees Vary in Engagement

Some boards house cybersecurity within the audit committee. Others have a dedicated cyber or risk committee. CISOs must know who owns cyber oversight and what materials they expect.

### 9. Board Members Are Often Curious but Uninformed

Many directors want to learn more about cyber but lack technical backgrounds. CISOs should embrace a mentoring mindset, offering plain-English education to build cyber literacy over time.

### 10. The CISO Role Is Becoming a Board Pipeline

As boards add cyber expertise, seasoned CISOs are being recruited as directors. Navigating the boardroom now may pave the way for future board membership.

## FINAL NOTE

In summary, public boards want to hear from CISOs, but they expect clarity, candor, and context. A well-prepared CISO can elevate both their company's risk posture and their own career trajectory.