HOW TO SPEAK THE LANGUAGE OF THE CORPORATE BOARD

DR. EDWARD AMOROSO

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

INTRODUCTION

Our many years of practical experience at TAG suggests that the corporate boardroom is just not a good place for technical acronyms, threat intelligence briefings, or deep dives into attack surfaces. Chief Information Security Officers (CISOs) who make attempts at such detailed discussions or jargon generally report bad results.

Keep in mind that we are not proponents of talking down to board directors, and we also do not believe the boardroom to be a good place for providing tutorials. Directors are expected to come to the board with experience, knowledge, and expertise. Briefings and communications are reasonable, but giving the rudimentary ABC-123's of any topic to directors seems improper.

That said, however, we do believe that if a CISO wants to gain support at the board level, then they must master the ability to speak in terms that directors can understand. This means shifting from references to detailed technical concepts to more mainstream references to risk, resilience, and return. Below are some recommendations on how this might be accomplished.

TEN RECOMMENDATIONS FOR SPEAKING TO BOARDS

1. Start With Business Impact, Not Threat Vectors

Boards don't want a lecture on ransomware mechanics; they want to know whether the business could be halted, or reputations destroyed. Frame issues around operational disruption, customer trust, and financial impact.

2. Use Simple, Clear Language

Avoid acronyms and technical phrases. Replace "EASM posture drift" with "exposure of unknown internet-facing systems." Your clarity reflects your leadership.

3. Align with Strategic Priorities

CISOs should show how cybersecurity enables key business goals like digital transformation, cloud migration, or M&A readiness. Security as a growth enabler resonates better than security as a compliance checkbox.

4. Quantify Risk When Possible

Use risk quantification techniques to communicate cyber exposure in dollars or percentages. For example: "This vulnerability introduces a $2.5M annualized risk based on likelihood and impact." This helps boards evaluate tradeoffs.

5. Tell Stories, Not Just Metrics

Case studies, analogies, or examples make cyber risks relatable. Rather than presenting "23,000 endpoint anomalies," say, "Last month, a misconfigured laptop led to unauthorized access."

6. Frame Cybersecurity as a Shared Responsibility

Don't position security as just an IT problem. Emphasize enterprise-wide accountability, including the board's role in setting tone, approving budget, and overseeing risk.

7. Leverage Comparisons and Benchmarks

Boards want to know how the company stacks up. Share peer comparisons, maturity benchmarks, or frameworks like NIST CSF to contextualize performance.

8. Know What Matters to Individual Directors

If a board member has a finance background, frame issues in budgetary terms. If a director has experience in operations, highlight supply chain resilience. Personalization earns trust.

9. Be Concise and Structured

Use a consistent format: risk, business impact, mitigation, ask. A three-slide deck with a focused message often works better than a bloated appendix.

10. Follow Up Proactively

Offer to brief individual directors or committees more deeply. Provide one-pagers or visual summaries they can revisit. This helps reinforce your credibility over time.

CLOSING COMMENT

In conclusion, CISOs who succeed in the boardroom are those who leave their technical hat at the door and adopt the perspective of a business executive. Speaking the board's language doesn't dilute the security message but rather amplifies it to those who matter most.