

Top 5 Considerations for Effectively Communicating Cyber Risk to Boards and Senior Management

01 Make it easy to consume.

- Use same format at each meeting: Dashboards / exec summaries
- Reference established framework, e.g., NIST, with trends over time
- Use 3-5 most important risk measurements, maturity indicators

02 Less jargon. More impact clarity.

- Translate technical terms/concepts into direct impact financials - a perspective that management and boards understand
- Express findings in terms of \$, business impact, reduced cost, etc.

03 Communicate improvement plans.

- Don't sugar coat it. Disclose gaps, but avoid doom and gloom.
- Provide assurances, e.g., we hit expectations here, we are short there
- Provide de-risk options by resource expense and priority

04 Organize around clear challenges.

- Make it obvious how to perform regulatory and cyber risk oversight
- Condense to threat risk - regulatory/non-regulatory, compliance gaps, lines of business maturity, cyber competency, etc.

05 Translate risk into benchmarks.

- Scale/scope, nation state vs. private, likelihood, impact, effort/cost/ROI to de-risk
- Reference exemplars - Boards will always ask "how do we compare?"