CISCO
SECURE

The bridge to possible

Talking to the Board

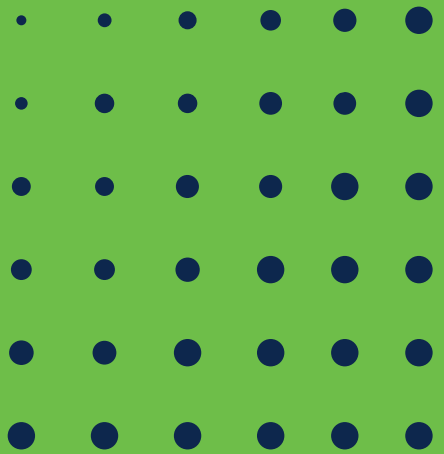
So The Board Will Talk Back

Helen Patton
Advisory CISO
June 2022

Agenda

- The Problem
- Roles and Responsibilities
- Engaging the Board
- What to Say, and How to Say It
- There Be Dragons
- What’s Next?

The ~~Problem~~ Opportunity



mis·com·mu·ni·ca·tion

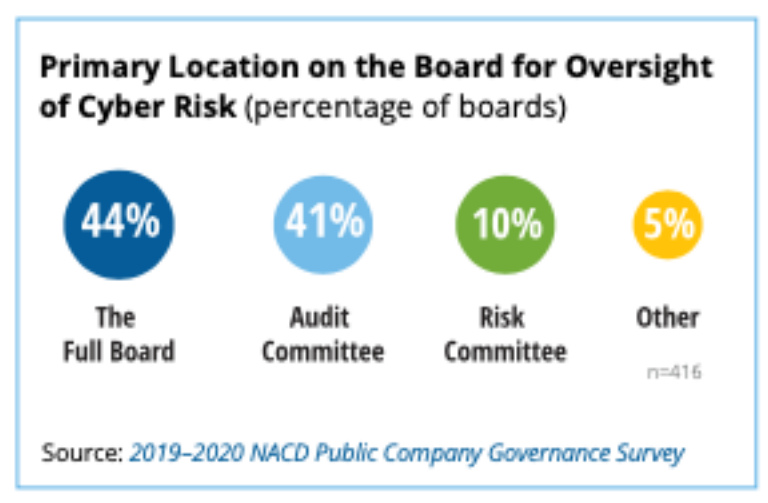
/ˌmiskəˌmyo͞onəˈkāSHən/

noun

failure to communicate adequately

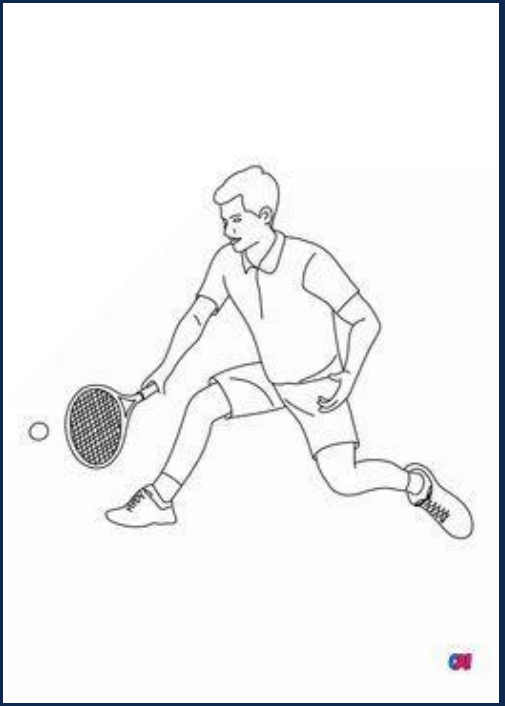
Board Members

- Don’t understand security, or systemic risks of technology - they recognize the risk, but don’t know how to quantify it
- Aren’t structured to pay attention to Cyber



Security Leads

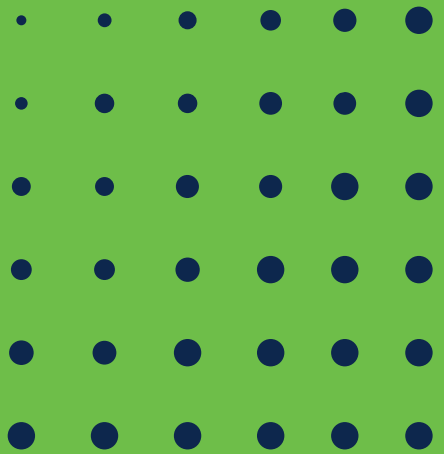
- Don’t understand how boards (should) work
- Don’t know what language to use
- Don’t have the right resources on the team



So What?

- Access to $$$
- Organizational Change Management
- Enable The Business
- Enhance Resilience

Roles and Responsibilities



“…include setting the company’s strategic aims, providing the leadership to put them into effect, supervising the management of the business and reporting to shareholders on their stewardship.”

The Cadbury Report (UK 1992)

Cyber Risk Corporate Governance

- Cyber is a strategic business enabler
- Understand economic drivers and impact of cyber risk
- Align cyber-risk management with business needs
- Ensure organizational design supports cybersecurity
- Incorporate cyber expertise into board governance
- Encourage systemic resilience and collaboration

World Economic Forum (Mar 21)

Cyber Risk Oversight

- Understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.
- Understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- Have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on board meeting agendas.
- Set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.
- …include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

National Association of Corporate Directors Handbook (2021)

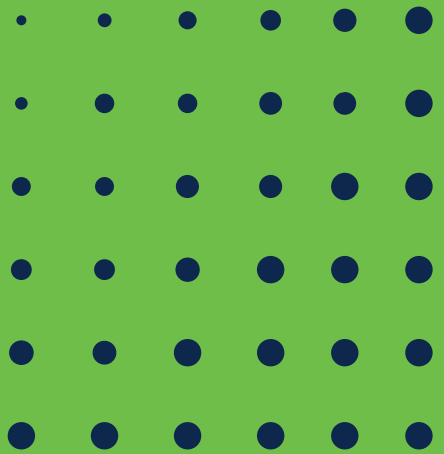
"The key questions for the board are no longer limited to how technological innovation can enable business processes, but how to balance their own major digital transformations with effective management of inherent cyber risk that can compromise the enterprise's long-term strategic interests."

NACD Handbook (2021)

"It is the job of a CISO to help the board of directors or non-technical members of the organization understand the security risks involved in their decisions for the company's current and future vision."

https://blog.eccouncil.org/what-is-ciso-roles-responsibility-career-salary-and-requirement-for-becoming-ciso/

Engaging the Board



How Are You Organized?

- Good:
  - Have a dedicated IT/Cyber Committee
  - Have technical SME Directors
  - Do regular full board reporting
  - Have 1:1/Independent access to Directors

?

- Less Good:
  - Have limited/no time with Board
  - Have cyber as part of the Audit Committee
  - Have gatekeepers to Director access

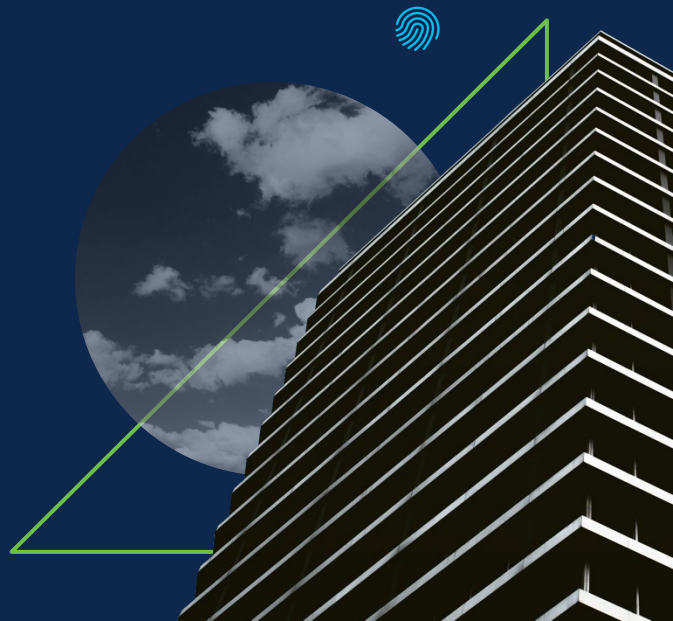
?

Establish a Relationship

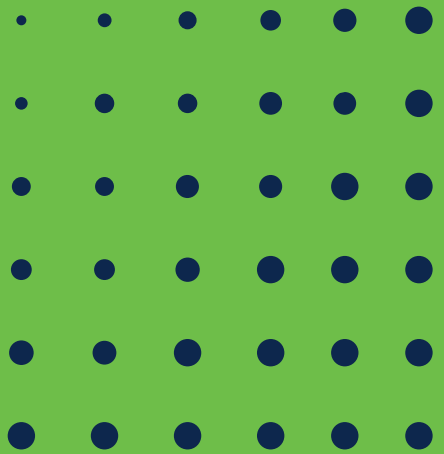
- Be part of new Director onboarding
  - Role/responsibility expectations
    - Normal business
    - Incidents
  - Set expectation for regular and off-cycle updates
- Offer White Glove Security Services
  - Director setup/data usage
  - Home/Family services

CISO-Director Activities

- Tabletop Exercises
  - Director-level role play
  - Director observation of Management TTX
- 1:1 Meetings w/ Key Directors
  - Regular (Quarterly?)
  - National/Industry Events
  - Conversation allowing questions
- Board Training
  - Raise general skills of Board
  - Understand company risk appetite



What To Say
And How To Say It



Formal Board Presentations

Photo by Elisa Ventur on Unsplash

Photo by Joshua Hoehne on Unsplash

Tell A Story…

Beginning

Middle

End

Tell A Story…

Where We Started

Middle

End

Tell A Story…

Where We Started

Where We Are

End

Tell A Story…

Where We Started

Where We Are

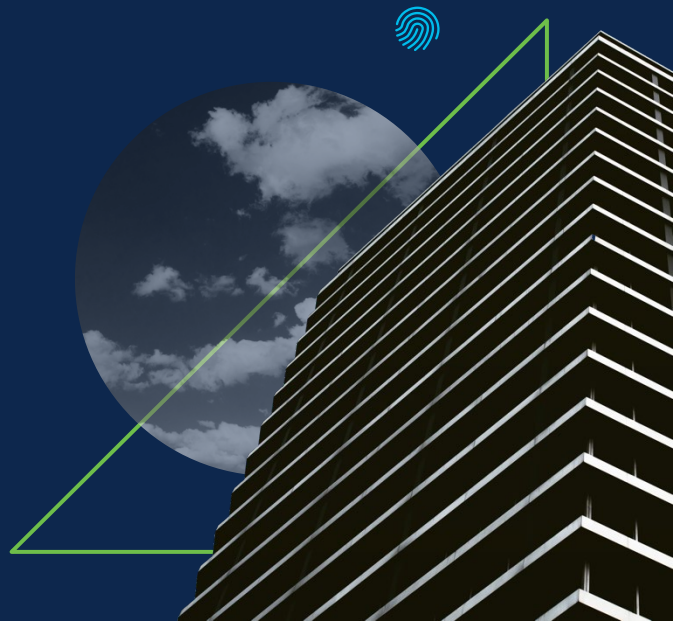
Where We Plan To Be

This Means…

- Frameworks to show maturity progression
- Third Parties to independently assess progress
- Speak of value at risk
  - AKA link to business objectives
- No technical metrics
- Benchmarking (or at least, peer comparison)
- Takeaway question…and action

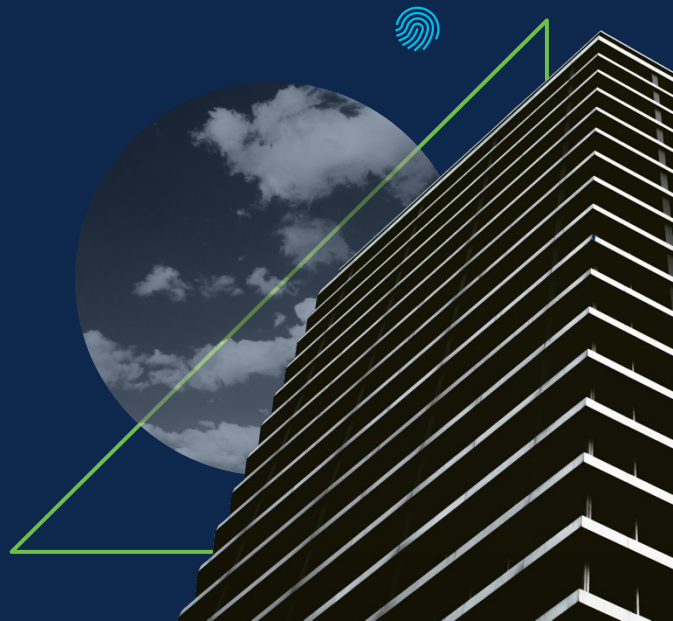
Questions for the Board

- Does This Match Your Understanding Of Our Risk Tolerance/Appetite?
- Is There Additional Clarity I Can Provide?
- What Would You Like To See In Future Reports?
- Would You Like to See A Different Outcome?

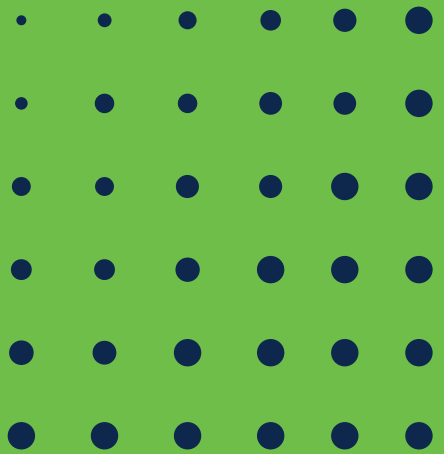


Board Actions

- Follow Up 1:1 Call To Further Explain Material
- Meeting with C-Suite to Deep Dive on Project/Initiative Risks
- Use of Board Concerns in TTX Scenarios



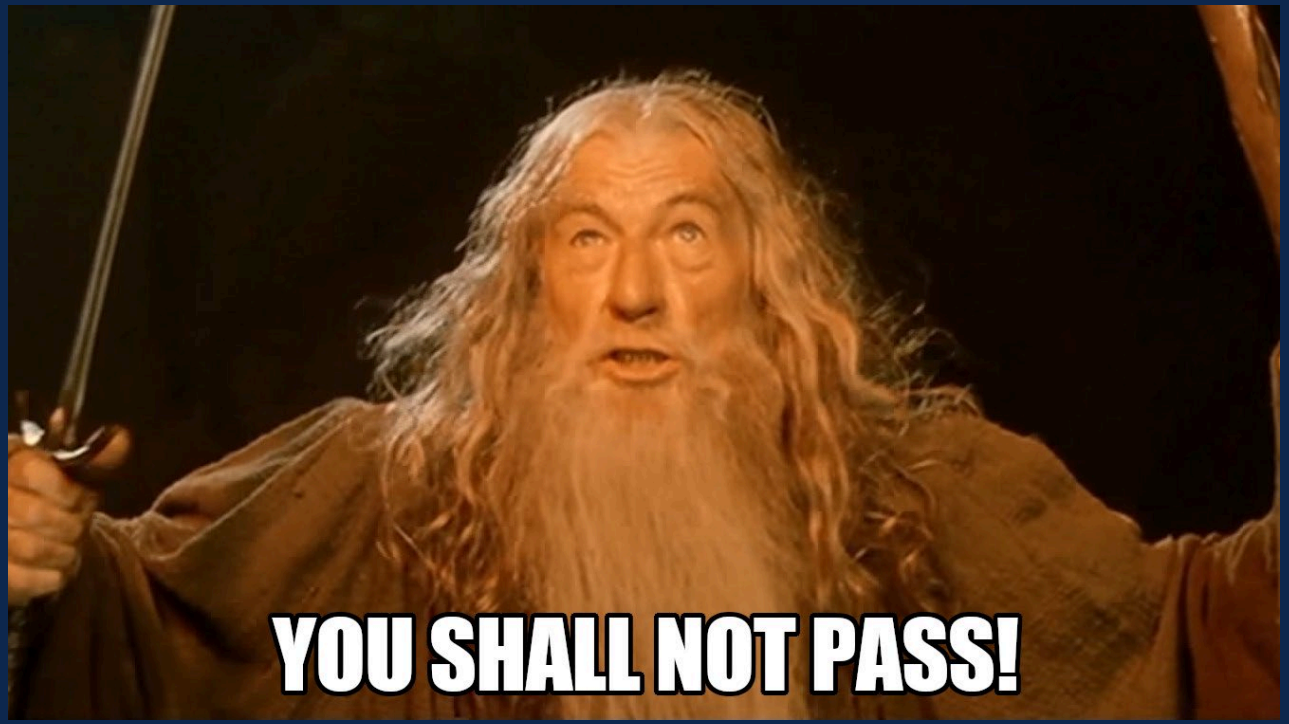
There Be Dragons



Delivering Bad News

Photo by Brett Jordan on Unsplash

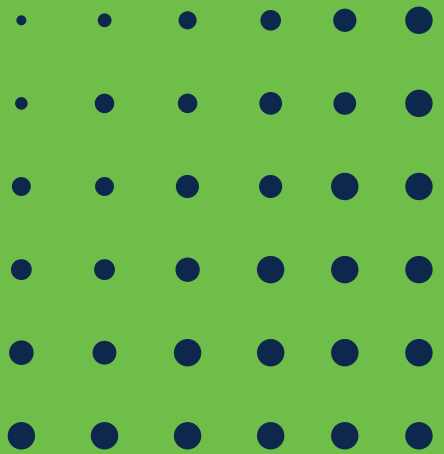
Managing Gatekeepers



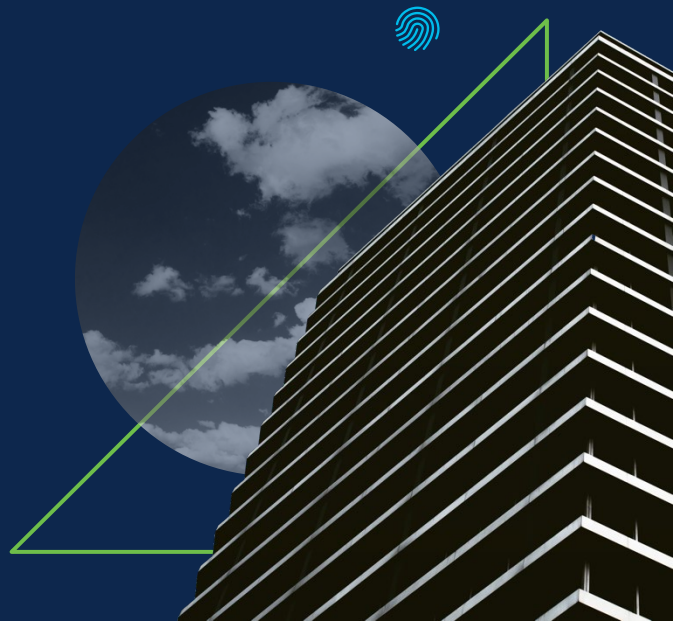
Don’t Do It Alone – Vendors/Partners

- Benchmarking
- External assessments
- Board exercises
- State of the industry
- Security teams of other Director organizations

What Next?



- Formal communication strategy
- Describe outcomes, not capabilities/products
- Talk in terms of business-aligned investments
- Tell stories, often




CISCO
SECURE