Engaging your Board on cyber security

Claudio Silvestri
Vice-President & Chief Information Officer
NAV CANADA
68% of Boards feel they are doing enough to support cyber security strategies.

Source: Harvey Nash / KPMG CIO Survey 2018 (3,958 surveys: 84 countries)
77% of CEOs feel prepared for a cyber incident.

Source: Harvey Nash / KPMG CIO Survey 2018 (3,958 surveys: 84 countries)
22% of CIOs feel prepared for a cyber incident.

Source: Harvey Nash / KPMG CIO Survey 2018 (3,958 surveys : 84 countries)
01 Know your Board

02 Board essentials
01

Know your Board
Know your Board

- Members and culture
- Priorities and risk tolerance
- Understanding of cyber security
- Operating level of detail
Does your Board take cyber security seriously?

- Regular agenda item?
- Lack of appreciation?
- Considers it a technology issue?
- Relies on management?
Where’s the gap?

- Difficult to maintain clarity
- Language often confusing
- Differing opinions on oversight
- Meaning of cyber maturity
Boards have a great sense of smell...
Board essentials
Define your threat landscape, your adversary and related trends
Assessments of how mature your process and technology are, the gaps, and how you compare to others.
Lay out your investment and initiative **roadmap** and what **strategies** it supports
Describe your capabilities across all related areas.
Describe your incident response plan and your return-to-service plan.
Describe how you will communicate internally and externally
High focus on employee awareness and education

“Trusting suspicious emails is a lot like eating yellow snow… ...you shouldn’t do either!”
Who will provide third-party **assurance** and how?
What is your approach to innovation?
What are your models for funding, resourcing, and skill development?
Thank you / Merci

Claudio Silvestri
Vice-President & Chief Information Officer
NAV CANADA
claudio.silvestri@navcanada.ca