ADVANCED CYBER SECURITY CENTER

Trusted Networks. Advancing Cyber Strategies.

Selected **Cyber Risk Governance** slides

ANNUAL CONFERENCE

Cyber Risk Governance

Leveling up in an Age of New Regulations and AI

Thank you

Strategic Partner & Lead Sponsor

ISTARI

Conference Sponsors

redsense
CYBER THREAT INTELLIGENCE

FOLEY HOAG

Our Host

FEDERAL RESERVE BANK OF BOSTON™

Today's Agenda

9:00-9:20	Welcome
9:20-10:45	**Cyber Risk Governance and Organization – Getting cybersecurity out of the box**
10:45-11:50	**CRG Table Discussions:** Cross-functional cyber risk governance discussions
11:50-12:25	Networking lunch
12:25-2:00	**The AI Juggernaut and Cyber Risk Governance**
2:00-3:30	**AI Network Breakouts:** Strengthening peer networks, unpacking AI opportunities
3:30-4:30	**Fireside Chat:** Threats, Responses and Federal Initiatives
4:30-5:30	Networking reception sponsored by Red Sense

ADVANCED CYBER SECURITY CENTER

Trusted Networks. Advancing Cyber Strategies.

Our Mission

The Boston-based ACSC **advances member cyber defense strategies** through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent.

ACSC Members

Financial Services
Manulife/John Hancock*
Munich Re*

Engineering/Industrials
Aptiv*
Schneider Electric*
VHB

Education
Harvard University
Northeastern University

Defense Non-Profit
MIT Lincoln Laboratory*

Government
Commonwealth of Massachusetts*

Healthcare/Life Sciences
Abacus Insights
Commure
ElevateBio
Point32Health
The Jackson Laboratory

Technology
Dell Technologies*
Everbridge
Mimecast
NetScout
Park Place Technologies
SmartBear Software
Tenable
Veracode

* Lead Partner

Founding Partners
Federal Reserve Bank of Boston
MITRE

Legal / ACSC Counsel
Foley Hoag LLP

ACSC Research Partners

Tapping innovative leaders to enhance the CISO challenge agenda, thought leadership in NDA covered convenings

Exercises

SIMSPACE

Cloud native security

aqua

tenable

Third party risk

BLACK KITE

ProcessUnity

Cyber GRX

Detection & response

THREAT WARRIOR

Governance & risk

CyberSaint SECURITY

and our new 2024 Research Partner

eclypses

ACSC's Three Readiness Pillars

Team Readiness

2023 Exercise Schedule

Table Top

October 17-18

Annual Table Top Exercise

Cyber Range

SIMSPACE

July 25-Aug 2

Wrap session August 3

Defender Challenge #1

September 18-21

Live Fire, Full Team Exercise

Nov 28-Dec 6

Wrap session Dec 7

Defender Challenge #2

January TBD

Wrap session January TBD

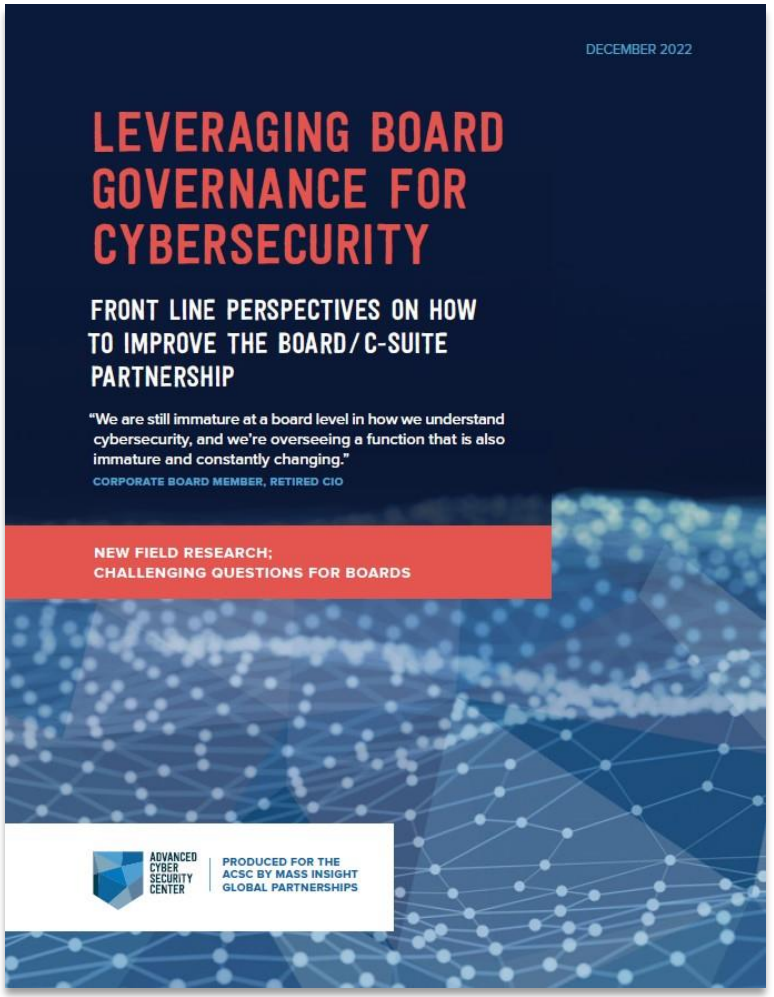
Defender Challenge #3

ACSC

Corporate Board Report

THE BOARD-MANAGEMENT STRUGGLE WITH CYBER RISK GOVERNANCE

The report was developed from interviews with 27 cybersecurity executives, risk officers, corporate Board members, and advisors and legal counsels



Cyber Risk Governance: Engaging Senior Management and Boards

A practice-sharing collaborative of CISOs, Risk Officers, Legal Counsels

Cyber Governance & Risk: Getting Ahead of the Regulators

Rob Knake, Principal Deputy National Cyber Director (acting), **The White House**

March 30 ✓

Managing & Communicating Cyber Risk as Business Risk: Priority-setting & Metrics

Lead organizations: **Harvard University** **Munich Re**

June 22 ✓

Cyber Insurance & Risk Management

Leads organizations: **Marsh McLennan** **State Street**

July 27 ✓

Embedding Risk in Strategic Decision-making

Lead organizations: **Schneider Electric** **Dell Technologies**

September 28 ✓

Cyber Risk Governance and Organization – Getting cybersecurity out of the box

Key participants: **All of you**

November 8

ACSC

Cyber Risk Governance Artifacts

Board Questions & Effective Board Engagement

Key Indicators of a Mature Cyber Organization

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

The message from Board members and advisors

"We are asking the same fundamental questions and getting the same bad answers…"

Board member, retired CIO

Three major factors driving the need for change

- New accountability for boards
- Increasing complexity (and risk) in the digital world
- The impact of CEO leadership

Board and CEO leadership drive the culture

"The importance of the Board's role in promoting a cyber-focused mindset and a cyber-conscious culture throughout the organization cannot be overstated."

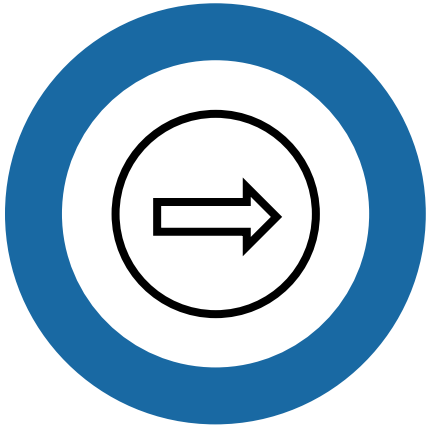
A New Chapter in Cyber – On The Board's Agenda | Deloitte, June 2022

Corporate Board Report framing elements

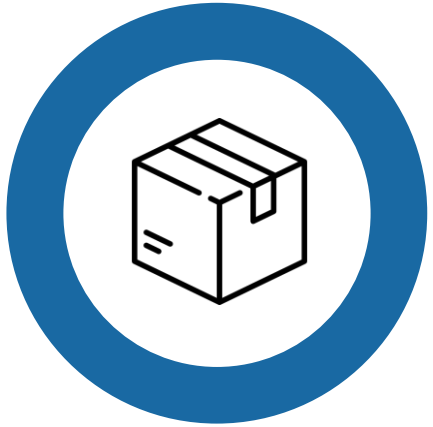
- The Board’s strategic risk role
- Cyber risk frameworks
- The evolving CISO role, management structures

The Board’s strategic risk role

Continuing disconnect



A one way conversation



Cybersecurity In a box

Cyber risk frameworks

- A **continuing challenge** – operational frameworks dominate
- New generation of **risk and resilience-based frameworks**
- Do we need a **GAAP for cyber**?

The evolving CISO role, management structures

"Companies still haven't clearly defined what their CISO does. If they did, it would be clear whom they should report to."

"There is an obvious tension between CIO/CISO priorities. Regulators care, does your board know that?"

But it's not all about the CISO – is cyber responsibility embedded across the organization?

The Board's three primary responsibilities

Board members should assure:

1. Cybersecurity risks have been incorporated into strategic business decisions, including mergers and acquisitions
2. A systematic risk framework and operational controls are in place, aligned with high priority risks and legal/regulatory/compliance requirements
3. Through continuous assessment and performance metrics, those programs are producing more security

ADVANCED CYBER SECURITY CENTER

Trusted Networks. Advancing Cyber Strategies.

Cyber Risk Governance
Board Engagement

Bob Nesbit
Defense Science Board

MITRE SVP – Center for Integrated Intelligence Systems (retired)

Larry Quinlan
Service Now
Board Director

Deloitte Global CIO (retired)

Incidents where attackers breach the network perimeter

1. Do you know who they were?
2. Do you know what they were after?
3. How far did they get before being detected?
4. What failed that allowed them to get this far?
5. What are you going to do about it?

As presented by Bob Nesbit

The previous example covered network security

*Beyond that, additional topics could be handled with the Board **in a similar fashion***

- How is employee access to the company's data and networks being managed?
- Have you carefully identified the company's most important assets and how well are they being protected?
- How resilient would the company be following a successful attack?
- What is the process we are using to prioritize cyber risks and allocate investments against our greatest risks?

As presented by Bob Nesbit

Suggestions for dealing with the Board on cyber security

1. Speak English.
2. Make it real. Nothing theoretical. Nothing bureaucratic.
3. Do not sugar-coat things.
4. Keep a constant format meeting to meeting.
5. Devise ways the Board can easily track progress.
6. Speak English.

As presented by Bob Nesbit

ADVANCED CYBER SECURITY CENTER

Trusted Networks. Advancing Cyber Strategies.

Cyber Risk Governance
The Risk Officer Perspective

Sonya Ross
Harvard University

Evan Wheeler
CapitalOne

Cyber risk is pervasive