ADVANCED CYBER SECURITY CENTER

CYBER RISK GOVERNANCE
Leveling Up in an Age of New Regulations and AI

Cyber Risk Governance
Conference Briefing Summary

November 2023

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED CYBER SECURITY CENTER

This Research

Digital risk (including AI) is getting more complex, boards are being held to higher standards of accountability, and top-down leadership on security and compliance is more important than ever.

Cyber risk should be factored in every major business decision. This Briefing Summary focuses on the strategic obstacles to making this happen and practical steps to improve cyber risk management and communication with boards. It's the product of robust, expert-to-expert presentations and discussions at the 2023 annual conference and earlier field research and case study briefings.

Thanks to these thought leaders

We'd like to thank the following leaders for their presentations at the November conference.

Larry Quinlan
Corporate Board member, ServiceNow, and Global CIO, Deloitte (retired)

Bob Nesbit
Defense Science Board leader and former MITRE Executive

Sonya Ross
Director, Risk Strategy & Financing, Harvard University

Evan Wheeler
Senior Director, Technology Risk Management, CapitalOne

Additional Resources
more detail on page 6

- Leveraging Board Governance for Cybersecurity Report
- Board Topics and Questions for Effective Governance
- Top Five Considerations for Effectively Communicating Cyber Risk to Boards and Senior Management
- Seven Indicators of a Mature Cyber Risk Organization

Contact us
(617) 584-0581
jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

Advice on building a culture and structure of collaboration

ACSC member executives understand the importance of working across traditional siloes and boundaries. Takeaways in this Briefing Summary focus on building collaborative and interconnected approaches to risk measurement and management across the organization.

Cyber risk is a shared business responsibility. Cyber risk is a pervasive feature of business that requires continuous collaboration across executive functions, balancing big picture vision with granular accountability that's best achieved through daily, proactive engagement.

"There must be a structure that allows the lines of business to take direct responsibility for their cyber risk posture and management. That's more important than where the CISO sits."

The CISO should think like a "Digital CFO". CISOs should work to properly frame challenges to the business, charting investments against expected returns and translating technical and security risks into financial language. Risk advisors give boards a different perspective, but it's up to the CISO to create a cohesive plan for framing the overall risk profile.

Frameworks don't magically drive collaboration. Frameworks are useful artifacts but can't always drive the right kind of collaboration. Some frameworks like FAIR are great for detailed operational risk but can overwhelm senior executives and boards with technical details, and they don't always communicate progress towards maturity.

"One of the foundational questions a framework cannot answer – are we investing to catch up or get ahead of threats?"

Leadership risk councils matter. Frequent engagement between leaders and risk teams is critical to nurturing trust and transparency across the organization.

"Our University Risk Management Council meets six times a year and incorporates cyber risk into its enterprise risk management."

Contact us

(617) 584-0581

jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

Insights on evaluating current board role and responsibilities

As identified in our *Leveraging Board Governance for Cybersecurity* report, boards and management have significant work to do in three areas as the SEC raises the stakes for the board's cyber risk governance.

1

Strengthening the board's strategic risk role

Boards need to sharpen how they listen and act. Too often, conversations are either one-way or at an inappropriate level of detail around either risks or solutions. Either result leaves boards disengaged and disempowered.

"We referred the cyber threat to the audit and compensation committee. If we want to get something done, that is where it goes."

2

Evaluating new kinds of frameworks

Increasingly interconnected risk requires an equally integrated response. This starts with finding the appropriate framework that's focused on outcomes like resilience and mirrors similar guidance to financial risk standards.

"The first thing a board needs is structure, a framework… tracked with metrics, with our plan and performance evaluated independently on a regular basis."

3

Rethinking corporate CISO role and management structures

Boards need to look at current corporate structure to understand where the CISO reports and if they have sufficient executive endorsement and autonomy to act. They need to design structures that ensure the CISO works directly with risk, legal, and the business while still keeping compliance strategy and operationalization separate.

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

Contact us

(617) 584-0581

jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

Guidance for effectively engaging boards

Consistent and effective board engagement is critical to getting executive support for cyber risk programs and priorities. We asked ACSC members for practical insights into successfully engaging key leaders.

what to do	what not to do
Get prepared well ahead of the meeting, working hard to anticipate every possible question	Don't "sugar coat" your report, present an objective picture of the cybersecurity strengths and gaps.
Reach out early, sharing material with board members and trying to assess what might matter most to them	Don't get surprised with questions or concerns from board members or stakeholders.
Keep it real by avoiding too much theory or technical language	Avoid letting the board take control by humoring every idea or concern they might have.
Try to be consistent in meeting formats and deliverables, which also makes tracking progress and challenges easier	Never be seen as condescending or to be ignoring ideas just because you think you know best.

Using after action reports to educate the board

After action reports can be useful tools for educating the board. They can help paint a complete picture of the threats and response by telling the full story of:

- Who the adversary was and how they got in
- How their activity was detected and mitigated
- What assets were compromised
- How these assets have been secured
- Costs and lessons learned from the incident

Contact us

(617) 584-0581

jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

ACSC's Mission and Research

The New England-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 is powered by a talented network of senior cybersecurity experts with leadership roles inside top public and private sector organizations. Through regular group discussions, surveys, tabletop exercises, and other efforts, ACSC draws on our members' deep knowledge and experience to produce actionable, relevant insights into the choices and challenges facing today's cybersecurity, risk leaders, and the boards they serve.

Resources

"Leveraging Board Governance for Cybersecurity"
- our Corporate Board Report -

- **Leveraging Board Governance for Cybersecurity**: ACSC and Mass Insight published report, developed from interviews with 27 cybersecurity executives, risk officers, corporate board members, and advisors and legal counsels.
- **Board Topics and Questions for Effective Governance**: As part of the Board Report, a program developed with board members and advisors to ensure boards are effectively governing cyber risk.
- **Seven Indicators of a Mature Cyber Risk Organization**: Developed from earlier research with McKinsey and Co and refined through the member-driven Cyber Risk Governance convenings in 2023.

ACSC Cyber Risk Governance Program Launch
March 2023, Foley Hoag
A collaborative of CISOs, CIOs, Risk Officers and Legal Counsels

- **Engaging the Board, Getting Ahead of the Regulators - March 2023 Briefing Summary:** Member priorities and recommendations for preparing boards and senior management.
- **Top Five Considerations for Effectively Communicating Cyber Risk to Boards and Senior Management** from the executive table discussions.

Contact us

(617) 584-0581

jdinneen@acscenter.org