GLOBAL cyber risk LLC

THE COUNCIL

The Council of Insurance Agents & Brokers

CIAB: The Council Academy

Director & Officer Liability: The Role of Cyber Governance

Jody R. Westby, CEO, Global Cyber Risk LLC

July 29, 2021

Council Academy: Exploring the Cyber Risk Environment

- 7/20/21 The Current Cyber Threat Environment & Actions to Take
- 7/21/21 Countering Cyber Attacks: What Good Incident Response Looks Like
- 7/27/21 Managing Cyber Risks Associated With The “New Normal”
- 7/28/21 Cyber Compliance: Here Come The Regulators And Lawsuits
- 7/29/21 Director & Officer Liability: The Role of Cyber Governance

Agenda

1. Drivers of Cyber Risk: Litigation and Regulators
2. Standard for Cyber Governance
3. Trends in Governance
4. Key Questions and Activities in Cyber Governance
5. Sample Organizational Structure
6. Characteristics of Cyber Governance
7. Summary

Regulators Are a Driver of Cyber Governance

- FTC placing more emphasis on management's involvement in privacy and information security.
- In January 2020, the FTC noted three major changes in future Orders:
  1. they would be more specific
  2. more third-party assessor accountability, and
  3. would "elevate data security considerations to the C-Suite and Board level."
- "Every year companies must now present their Board or similar governing body with their written information security program — and, notably, senior officers must now provide annual certifications of compliance to the FTC."
- SEC in 2014 told boards "there can be little doubt that cyber risk also must be considered as part of the board's overall risk oversight."
- In 2018, SEC Chairman Jay Clayton noted that cybersecurity was one of the three key market risks for public companies that the SEC was monitoring and expanded previous guidance.
- FFIEC has set forth detailed governance obligations for financial institutions
- New York Department of Financial Services – requires senior official certify compliance with cybersecurity requirements
- National Association of Insurance Commissioners Model Law on Data Security with similar provisions

Manage Risks Through Cyber Governance

- Governance structure is needed at board and senior executive levels that enables proper oversight of key risks and vulnerabilities and ensures executives and directors receive timely and important information about these risks.

- **ISO/IEC 27014 Governance of Information Security:**

"Governance of information security provides a powerful link between an organization's governing body, executive management and those responsible for implementing and operating an information security management system. It provides the mandate essential for driving information security initiatives throughout the organization."

- Laws and regulations also require governance: HIPAA, FISMA, FTC, FFIEC, SEC, NYDFS, NAIC

- Cyber Governance is really:

Compliance + Protect Data & Processes + Cybersecurity Program = Risk Management

Cybersecurity Governance Standard: ISO 27014

ISO 27014 Governance Objectives

6 Objectives

1. Information security objectives should be integrated across the entity
2. Information security decisions should be made using a risk-based approach
3. Information security risks should be evaluated for acquisitions, new investments, mergers, adoption of new technologies, etc.
4. Information security policies and procedures should align with operational and external requirements
5. Governance of information security should be built on a positive culture of cybersecurity
6. The performance of the security program needs to match current and future operational needs.

Trends in Cybersecurity Governance: 2015 Governance of Cybersecurity Report

- In 2015, the percentage of boards actively addressing and governing computer and information security nearly doubled from previous surveys (63% v 33% in 2012).

- For the first time, the survey indicated that more boards are regularly or occasionally engaged in every area of governance best practices related to privacy and security.

- Some of the biggest improvements over time have been organizational
  - 53% of boards have a Risk Committee, up from 8% in 2008
  - 79% of respondents have a cross-organizational group to manage privacy and security issues, up from 17% in 2008.

- For the first time in all four surveys, the 2015 responses indicate the Risk Committee has the most responsibility for the oversight of risk, overtaking a role long held by the Audit Committee.

- The financial sector continues to live up to its reputation of having the best security practices, having the highest percentage of board involvement in every best practice area except reviewing privacy and security roles and responsibilities.

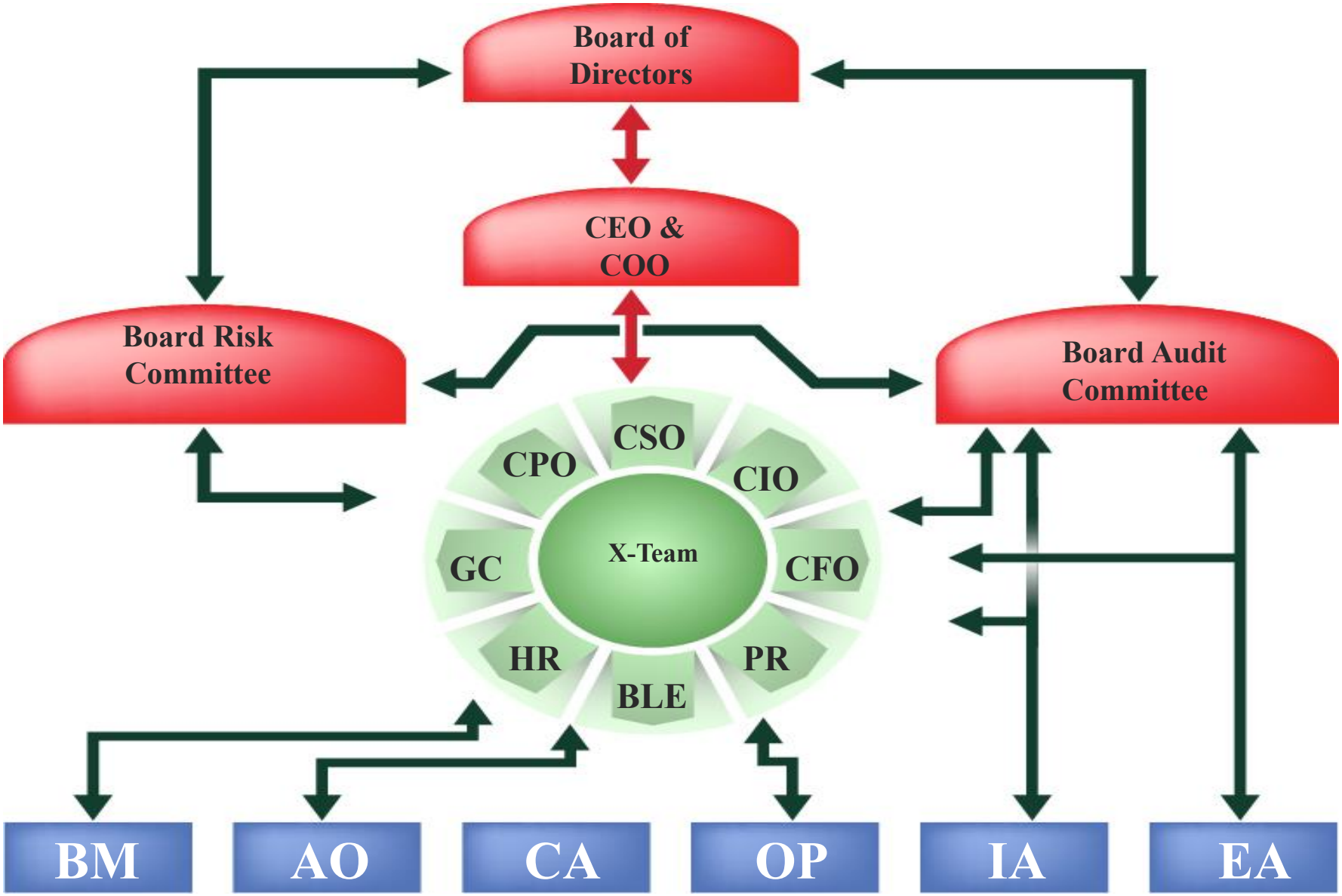
Governance Actions: The Bottom Line

- Develop a governance framework in alignment with best practices and standards
- Identify key risks to operations & monitor those risks
- Ensure privacy and security compliance requirements are met
- Ensure the organization's cybersecurity program is mature & in alignment with best practices and standards
- Review information flows on risks and monitor operations and compliance
- Ensure incident response plan and BC/DR plans are developed & tested
- Develop appropriate risk transfer and management strategies
- Review annually against operational changes, new laws/regs, and changes to threat environment

Beginning Governance Questions

- What are your organization's key vulnerabilities, internally, with vendors and other providers?
- Does your organization have an enterprise security program that meets best practices and standards? Is it mature?
- Does your security program integrate compliance requirements?
- Do you know where there are gaps & deficiencies in the program and what remediation measures are needed? Are they budgeted and planned?
- What would be the financial consequences of a significant breach or cyber event?
- Are you prepared to manage a major event?
- What types of insurance coverage does the organization need and what limits?
- Are your executives and board exercising governance over privacy and security risks per governance standards and legal requirements?

Sample Governance Structure



Roles & Responsibilities Between Board & Executives

- Separate roles and responsibilities between board and executive suite
- Board role focused more on reviews, approvals, evaluations, allocation of resources
- Executive role more on alignment, establishing, developing, informing, supporting
- identification of vulnerabilities that could have a material impact on corporate operations and/or bottom line
- Utilize outside expertise to help stay abreast of threats, provide independent view & coordination of incidents; conduct annual review of alignment of security and business strategy, business requirements, compliance

Effective Governance Characteristics

- Security managed as enterprise issue
- Leaders are accountable
- Security viewed as business requirement
- Risk-based (compliance, operational, reputational, financial)
- Roles & responsibilities defined with segregation of duties
- Security addressed & enforced in policies
- Adequate resources committed to security program
- Staff aware & trained
- Security addressed throughout system development life cycle
- Security is planned, managed, measured & weaknesses addressed
- Annual reviews & audits
- Risk transfer strategy based on operations and financial data
- D&Os have info flows on risks and status of above and monitor / manage

Exercising Cyber Governance

1. Establish governance structure
2. Understand specific cyber vulnerabilities associated with operations
3. Identify key information flows & reports to inform board & executives
4. Identify legal compliance and financial exposures from IT systems
5. Set tone from top and approve top-level policies on privacy & security risks
6. Review roles & responsibilities of lead privacy & security personnel & SOD
7. Ensure that privacy & security responsibilities are shared, enterprise issues
8. Know the security activities over which boards need to exercise oversight
9. Review and approve annual budgets for security programs
10. Review annual risk assessments & support continual improvement
11. Retain trusted advisor to inform on changes in threats, assist governance
12. Evaluate the adequacy of cyber insurance against loss valuations

GLOBAL cyber risk LLC

Summary

- Cyber governance is now a requirement; it involves more than asking interesting questions
- D&O lawsuits, regulatory action, and headlines are realities
- Failure to meet ISO standard for information security governance, comply with legal requirements, and establish internal governance framework creates high risk
- Define roles and responsibilities and know what actions to take, what risks to monitor, and what information flows are necessary.
- Consider having a trusted advisor to the board on these issues.

CIAB Resources from Leader's Edge

- Ripple Effects of Cyber Attacks, June 1, 2021, https://www.leadersedge.com/p-c/ripple-effects-of-cyber-attacks
- Cyber Caveat Emptor, May 2, 2021, https://www.leadersedge.com/p-c/cyber-caveat-emptor
- Leadership, Training, Controls, Aug. 25, 2020, https://www.leadersedge.com/p-c/leadership-training-controls
- Trust in Data Can Be a Competitive Advantage, July 16, 2020, https://www.leadersedge.com/p-c/trust-in-data-can-be-a-competitive-advantage
- Forgiveness After An Attack, Jan. 14, 2021, https://www.leadersedge.com/p-c/forgiveness-after-an-attack
- 2020 vs. 2021, Nov. 30, 2020, https://www.leadersedge.com/p-c/2020-vs-2021
- You Thought COVID-19 Was Bad, Sept. 24, 2020, https://www.leadersedge.com/p-c/you-thought-covid-19-was-bad
- 20 for 2020, Jan. 14, 2020, https://www.leadersedge.com/p-c/pay-now-or-pay-later
- Risk Assessments Are The Best Checkup, Oct. 28, 2019, https://www.leadersedge.com/writer/jody-westby
- Managing Risks in an Industrial Control Environment, Sept. 27, 2019, https://www.leadersedge.com/p-c/managing-cyber-risks-in-an-industrial-control-environment

Thank You!