Excerpted from ***Leveraging Board Governance for Cybersecurity*** – published December 2022 by the Advanced Cyber Security Center and Mass Insight Global Partnerships

BOARD QUESTIONS & EFFECTIVE BOARD ENGAGEMENT

ADVANCED CYBER SECURITY CENTER

PRODUCED FOR THE ACSC BY MASS INSIGHT GLOBAL PARTNERSHIPS

© 2022 Advanced Cyber Security Center (ACSC) and Mass Insight Global Partnerships

A PROPOSED PROGRAM

3 Strategic Oversight 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

Board advisors, legal counsels and experts interviewed stressed that Board members must be able to demonstrate to themselves and regulators that they are challenging management. Despite traditional norms dictating minimalist Board minutes, there were suggestions that with new regulatory scrutiny, Board minutes for highly regulated firms will need to demonstrate that challenging discussions occurred.

Board "due care" for cybersecurity means taking reasonable steps to secure and protect assets, reputation, and finances. Recent Delaware court decisions have called upon directors to "ensure that companies have appropriate oversight systems in place."

Regulators are raising the stakes for Boards:

> "Regulators ask, what are you doing? Show me the investments and what has improved. Show me the management process to prioritize your investments. The Board must demonstrate that they are able to challenge the CISO — not sure Boards are listening."
>
> BOARD ADVISOR

Boards must understand/question risk frameworks, process controls, decisions about security investments:

> "As a Board member, I can't and shouldn't review every process control you are using but: What is the risk management system at the control level that you have put in place and how do you know it's working? I want to know management thought this through and has a system with metrics attached to it."
>
> BOARD MEMBER

> "What are the 10 most fundamental business processes that have existential connection to business outcomes? Are our security investments directly linked to those 10 processes?"
>
> SENIOR DATA OFFICER

Boards need evidence that the CEO and COO are personally driving a security culture:

> "How often are digital risks viewed and managed in the governance structure? How often is it discussed at senior management level?"
>
> BOARD ADVISOR

> "Talent gaps: Boards should ask about them. Most organizations have significant skills and capacity weaknesses and don't raise this with Boards. Where are we weak, how are we covering for that, are we compensating with vendors?"
>
> BOARD ADVISOR

Advisors and legal counsels cautioned: Board members will be unable to fulfill their oversight responsibilities without a full understanding of current compliance posture, as well as assessing current risks and strategic operational decisions.

5 Lines of Board Questions

Corporate Board members and advisors proposed five key lines of questioning for management:

1. Compliance with legal and regulatory requirements — today and planning for the future

- **A comprehensive review and plan:** Are we satisfying our legal, regulatory and compliance obligations in every jurisdiction and planning for future requirements?
- Does our broader business and technology roadmap account for emerging cybersecurity issues and legal requirements, including risks of AI, for example?

2. Managing strategic digital security risk as business risk

- **Strategic risk and business planning:** Are cybersecurity and/or risk officers at the table for enterprise strategic planning — and for mergers and acquisition decisions?
- **Risk frameworks and controls:** What are the fundamental business processes supporting our business outcomes, the risk framework and management system at the business process and control level and the metrics to track performance?
- **Risk transference:** What risks have we transferred — contractually to third parties, through cyber insurance?
- **Third parties:** What is our level of reliance on third parties — who are our most critical partners?
- **Risk in an agile environment:** What are we doing to respond to an "agile" decentralized control environment and remote work? How are we implementing zero trust?
- **Risk level agreements:** Have we put in place risk level agreements that confirm shared cross-functional executive risk responsibilities?
- **Risk acceptance:** What risks are we accepting — are we comfortable with those?

3. Security culture, organizational structure and the CISO role

- **Management security culture:** How are we communicating business responsibility for digital risk?
- **CISO role:** What are the CISO's defined responsibilities? How have we resolved the inherent conflict where CISOs have both policy/assessment and operational responsibilities if we do not have three lines of defense (business/IT, risk policy/assessment, internal audit)? Does the CISO have both the necessary authority politically and the visibility into broader technology/enterprise programs required to secure them?
- **CEO/COO leadership:** Does our CEO or COO lead a cross-functional executive council or regular review sessions to oversee cybersecurity and business continuity risk management and performance on at least a quarterly basis?
- **Executive responsibilities:** Are there digital risk performance requirements C-Level executive jobs?

> "CISOs — many of them — and Boards are ignorant about legal/regulatory risks, which creates blind technical risks, so the board doesn't know what they don't know — they can't possibly ask the right questions.
>
> CISOs must learn to translate all operational risk into business continuity/financial risk — what parts of the business are affected if they have a problem."
>
> CORPORATE BOARD ADVISOR

Board Questions — Continued

4. Business continuity and resilience, planning and simulations

- **Simulations:** What incident simulations have we run — e.g. Ransomware, insider threat — and what corrections have we made based on them? Are Board members participating?
- **Shifting from continuity to resilience:** What systems are/aren't going to be operational in the face of attack? What have we done to compensate for those losses?
- **Business disruption target:** What is our maximum acceptable time offline for our most important business processes, and the financial impact associated with cyber incident scenarios?

5. Continuous performance assessment of people, process and technology

- **Strategic security investment bets:** Where have we over-weighted investment to defend against our most significant, existential threats/risks and how are we measuring the value of the additional investment (threat intel, 3rd party risk, new detection tools and programs)?
- **Framework:** What is our risk framework, what was the process to design it, are you confident it works — and why?
- **Benchmarks:** What is our benchmark for cybersecurity/business continuity performance — externally with peers or internally against business controls or both? What are our business continuity metrics?
- **Unsupported systems:** How many legacy systems do we have, how are we patching, what's our plan?
- **Defender team assessments:** Are we conducting red team, "live fire" exercises with our defender teams and benchmarking performance — are they improving? Can we benchmark performance against peers?
- **Talent and skills gaps:** With talent shortages in the market, what are greatest talent and skill gaps that threaten our security and business continuity — how are we covering for those with

Comprehensive industry resources on the role of Boards in cybersecurity include:

•National Association of Corporate Directors (NACD) Handbook on Cyber-Risk Oversight (2020 Edition)

•NACD Cyber-Risk Oversight Resource Center