Critical Do's and Don'ts of Cyber Risk Board Reporting

James Lam
President – James Lam & Associates
office: 781.772.1961
james@jameslam.com
www.jameslam.com

The three deadly sins

1. **Don't do stupid**. Risk assessments and heatmaps as commonly practiced are flawed. Risk identification and brainstorming should not be considered risk assessment.
2. **Don't do lazy**. Risks are the variables that drive performance. They are not the inability or failure to achieve a business objective.
3. **Don't do boring**. Corporate directors & executives want your perspectives and insights, not the processes and minutia of your work.

Fiduciary duties of corporate boards

- **Duty of Care.** Directors are required to:
  - Act with the diligence and competence of a reasonably prudent person in a similar position under like circumstances.
  - Avail themselves of all material information reasonably available to them.
- **Duty of Loyalty.** A director must in good faith (honestly) believe that he or she is acting in the best interests of the corporation and be free from conflicting personal interests.
- **The Business Judgement Rule** protects directors from liability when they act reasonably, in good faith, and on an informed basis.
- **Recent case law** has increased board awareness of standards for risk and compliance oversight (see Marchand v. Barnhill and Clovis Oncology derivative litigation).

NACD 5 Principles of Cyber Risk Oversight

1. Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

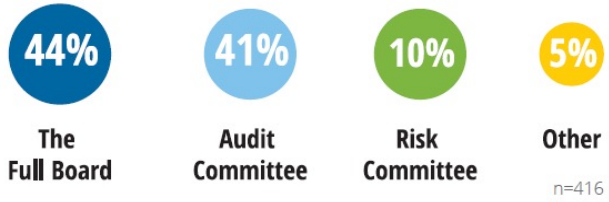
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

5. Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

Source: *NACD Director's Handbook on Cyber-Risk Oversight 2020*

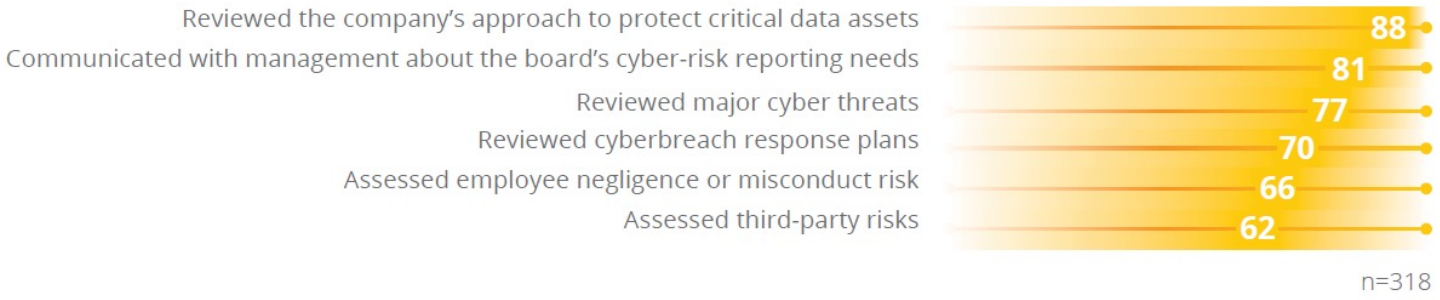
Board oversight of cybersecurity

Primary Location on the Board for Oversight of Cyber Risk (percentage of boards)



Source: *2019–2020 NACD Public Company Governance Survey*

Cyber-Risk Oversight Practices Performed Over the Past 12 Months (percentage of boards)



Source: *2019–2020 NACD Public Company Governance Survey*

Effective board-level cyber risk reporting (aka The "Wow" Report)

- Executive summary from the CISO
- Threat environment
- Independent cyber risk assessment and metrics
- Internal cyber risk assessment and metrics
- Quantification of cyber risk profile: past, current, future
- Oversight of cyber security and insurance strategies