What Directors Should Know About Cybersecurity and Risk Management

Catherine A. Allen
Chairman and CEO / The Santa Fe Group
Shared Assessments Summit / April 29, 2015
Hot Topics for Boards

- Oversee strategic planning in the face of uneven economic growth and rising political tensions
- Oversee cybersecurity as hackers seek to infiltrate even the most sophisticated information security systems
- Assess the impact of advances in technology and big data on the company’s business plans
Hot Topics for Boards Continued

- Cultivate shareholder relations and assess company vulnerabilities as activist investors target more companies
- Consider the impact of M&A opportunities
- Oversee risk management as newer and more complex risks emerge
- Ensure appropriate board compensation in light of increasing focus on diversity, director tenure and board size
Hot Topics for Boards Continued

- Explore new trends in reducing corporate healthcare costs
- Set appropriate executive compensation
- Ensure the company has a robust compliance program as the SEC steps up its enforcement efforts and whistleblowers earn huge bounties

*Directors and Boards, First Quarter 2015
Trends Driving Need for Better Board Oversight

- Regulatory pressure
- Reputational risk
- Changes in management and Board composition as result of increased risks
- Velocity of change in cyber crime and breaches
- Public awareness
- Growth in nation state espionage
- Growth of the “Internet of Things”
Trends Driving Need for Better Board Oversight

- Investors are demanding transparency
- Global shifts in outsourcing
- Increased Board education focused on third party risk
- Disruptive technologies and business models
Third Party Risk Market Landscape

- Heightened regulatory expectations
- Third party breaches dominate the news
- Expanded need for governance models
- Skill set gaps / lack of knowledgeable candidates for third party risk
- Need for efficiencies and cost savings
Critical Targets

- Financial institutions, including banks and brokerages
- Retailers
- Healthcare organizations and insurers
- M&A, advisory and law firms
- Electric utilities
- Other public utilities
- Manufacturing
- Smaller firms and vendors as entry point to larger organizations
What Boards are Doing

- Moving risk and cyber issues from audit to a risk or technology or security committee of the Board
- Supporting ERM programs
- Bringing on a Digital Director
- Getting educated internally and in corporate Board education venues
- Having frequent presentations on risk at the Board level
- Creating CISO independence
- Focusing on data governance and “Crown Jewels”
- Focusing on resiliency
Questions Boards Should be Asking

- Are the resources adequate?
- Do we have the right talent?
- What are the organization’s “Crown Jewels”?
- What is our risk appetite?
- Do we have a crisis management team and messaging in place?
- Do we have cyber and other risk insurance?
- What technologies are in place?
- Are we assessing our third party providers?
When Should the Board be Worried?

- When management is overconfident
- When there are overly-complicated and vague answers to questions
- When issues are not brought up or anticipated… look for outliers
- When the CISO says, “Don’t worry, we are totally secure”
- When not enough resources are in place
- When the company is outsourcing to new countries
How to Communicate with Boards

- Run presentations by the Risk Committee Chair and develop a close relationship
- Keep it focused on the business and related risks, not on the technology
- Present at Board committees as well as at Board meetings
- Send articles and updates between meetings
- Suggest outside experts to speak to the Board
- Find ways to summarize or use dashboards and have details in the appendix
Risk Management Dashboard

- Must identify key risks for all areas of the business with updates
- Must include probabilities, reputational risk and value to the company
- Must identify management and Board committee oversight and ownership
- Must include trends and opportunities
- Must include risk factors and response plans with metrics
- Must be color-coded
Questions?
About the Santa Fe Group

The Santa Fe Group is an internationally-recognized strategic consulting company providing unparalleled advisory services to Boards of Directors, leading financial institutions, healthcare organizations and other critical infrastructure companies.

The Santa Fe Group also manages the multi-industry Shared Assessments Program that provides comprehensive, member-focused tools and training to manage third party risks and relationships. Shared Assessments is a trusted forum for dialogue and collaboration among all stakeholders on issues that matter to outsourcers, their service providers, assessment firms, regulators and others.

Catherine A. Allen
Chairman and CEO, The Santa Fe Group
cathy@santa-fe-group.com