Diligent

Bringing the Board Up to Speed on Cybersecurity

5 Steps to Increase Directors’ Cyber Literacy

By Betsy Atkins

Under current reporting frameworks for public companies in the United States, no disclosures explicitly regarding cybersecurity are required. Yet that will soon change, and the U.S. director community will quickly need to perform cyber oversight in a differentiated way to comply with proposed SEC regulations expected to be finalized and announced in April 2023.

The Importance of Improving Boards’ Cyber Literacy

As boards begin the journey to cyber compliance, one of the first things they need to do is bring all members to a common understanding of the technology landscape. Everyone on the board needs to be familiar with and understand commonly used cybersecurity terms, concepts and frameworks, so that directors can correlate them to the economic decisions the board will be making to protect the enterprise.

Roughly speaking, there are five aspects of cyber readiness, all of which the board must be aware of:

1. Cyber training for all employees
2. The in-house cyber team (often led by a CISO)
3. The implementation of cyber software tools which protect the attack surface, ranging from the perimeter firewall to sensitive data to the company’s core IP
4. External cyber penetration testing by an outside firm
5. Potential engagement with an external security monitoring service

In terms of immediate actions, we need to start with board education to bring everyone to the same cyber literacy level. We also need to assign which committee is going to own cybersecurity oversight. Boards must also ask themselves, “How ready are we to comply with the SEC regulations? Where are the gaps?”

Additionally, we as board members should understand what the costs are and the budget impact of bringing our cyber systems up to a level that correlates to the cost and risk tradeoff of what our company can accept as the possible loss for our business. Every industry will have different areas of emphasis. For example, protecting intellectual property may not be as big an issue in a retail business as it is in a pharmaceutical business.

What follows are five steps for educating the board to perform cyber oversight in a way that not only complies with the SEC's upcoming regulations, but empowers greater performance by the organization, with less risk.

Step 1: Understanding the NIST Framework

One of the most basic foundational tools that is widely accepted and recognized for performing cyber oversight, and that boards need to understand, is the NIST framework.

The NIST Cybersecurity Framework, issued by the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce, is an oversight tool that breaks cyber risk into five categories and reviews the corporation's cyber posture and readiness to protect the corporation from a cyberattack. This ensures that the appropriate methodologies, software tools and personnel are in place. The NIST framework is often used by boards as a scorecard tool to review cyber resilience and readiness, and to rate and identify areas of strength and areas for concentration of resources to improve.

According to NIST's online learning resource, the NIST Cybersecurity Framework consists of three main components:

- Framework Core
- Implementation Tiers
- Profiles

The Framework Core consists of three parts: Functions, Categories and Subcategories. There are five high-level Functions: Identify, Protect, Detect, Respond and Recover. These five Functions are not only applicable to cybersecurity risk management, but also to risk management at large. In the next level down are the 23 Categories that are split across the five Functions.

The image to the right depicts the Framework Core's Functions and Categories.

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

The Categories were designed to cover the breadth of cybersecurity objectives for an organization, while not being overly detailed. They cover topics across cyber, physical and personnel, with a focus on business outcomes.

In my research I found that NIST has released the "Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework," which outlines potential significant changes to the Cybersecurity Framework for public review and comment. Management teams will likely want to ask their IT teams to study the proposal.

Actions for Boards:

□ Directors will be well served to do a review of the NIST Framework with the full board.
This way the entire board has been briefed. You can then report this in your proxy and other documents.

□ Questions directors may want to raise with their CISOs:

- What does the CISO consider the biggest risks for the business?
- Which risks are the biggest vulnerabilities and most likely to happen?
- Where is the vulnerability with the highest financial impact?
- What is the CISO's recommendation for prioritizing the most essential areas for investment?

Step 2: Understanding Cyber Breach Response Protocol

The natural next step is having a cyber breach response protocol in place.

Think through the protocol in advance. Have the IT and/or cyber teams review the crisis management tabletop exercise they have run with the board. Ensure that they're ready with external cyber forensic experts.

Actions for Boards:

□ As part of tabletop cyber planning, ask the CISO and/or tech team to run you through their post-breach protocol.
For example, who is the outside council they would use? Who is the forensic consultant? Who on the communications team is in charge?

□ Additionally, the FBI has an organization called the ISAC (Information Sharing and Analysis Center). ISAC can tie together different attacks from different cyber criminals and help inform your company's response. Be sure that your security team has a local contact at the ISAC. A good place to start is the FBI field office cyber supervisor.

Step 3: Determining Materiality and Reporting a Breach

The proposed SEC regulations will require disclosure of a material cyber incident within four days. Once a breach occurs, the clock has started. Ask yourself, "How prepared are we to do a materiality assessment and report?"

It becomes imperative that the board have a management plan for assessing materiality. This means that management needs to develop a new protocol for assessing cyber materiality. Ask management if there's someone designated from the finance and IT teams to think through what some bracketed levels of materiality would be. Is there an expert at your law firm and at your outside accounting firm that should be part of this cyber materiality assessment?

Actions for Boards:

□ Ask the right questions of management's materiality assessment framework, such as:

- What data loss or encrypted file lockout would have the biggest financial impact on our business?
- Are we able to understand if this is deliberate sabotage?
- Is it extortion or is it data theft?

Step 4: Seat a Cyber Expert in the Boardroom

Another component of the proposed new SEC regulations is that company boards will need to have a cyber expert and will need to disclose the directors' cyber credentials. In order to be considered an expert, a director will need to have clear cyber credentials: e.g., a clearance, experience working for a cyber security firm or in IT, or completion of adequate coursework.

Actions for Boards and Management:

□ The board may want to consider bringing in outside experts to give the entire board an orientation and briefing. Examples of external advisors include cybersecurity forensic firms, as well as outside accounting firms and outside law firms. I'm sure all boards are identifying which board members have cyber credentials and encouraging the rest of the board to quickly upskill in cyber issues.

□ Management may want to look at augmenting the IT and/or cyber team with external security managed service providers (MSP). MSPs add a level of independent 24/7 dedicated cyber monitoring that is often far more comprehensive than most corporations can afford.

Step 5: Prepare for Proxy Season

The SEC has required regular and periodic updates on corporations' cyber processes and policies. When the proposed SEC regulations are passed, this will become even more critical.

When it comes time to do your proxy, I recommend disclosing more rather than less.

Actions for Boards:

□ Address the following in your proxy statement:

- Describe exactly how your board is performing cyber oversight
- Identify who in management presents to the board on cyber matters
- State whether there are independent outside expert presenters
- State what your review is based on; e.g., the NIST framework
- Provide an overview of your company's IT and cyber organization, and where it reports

- Enumerate some of the areas you delved into, such as review of software, security software, training of employees, penetration testing and third-party monitoring services

- Clarify whether the whole board was trained, or if only certain members have received cyber training

- Identify any cyber credentials your members have, detail how the board is briefed, and how often it is briefed, on any risk around security

- Explain how you are thinking about the materiality to the business of cyber risks

- Explain whether you have a protocol in place to respond to a breach

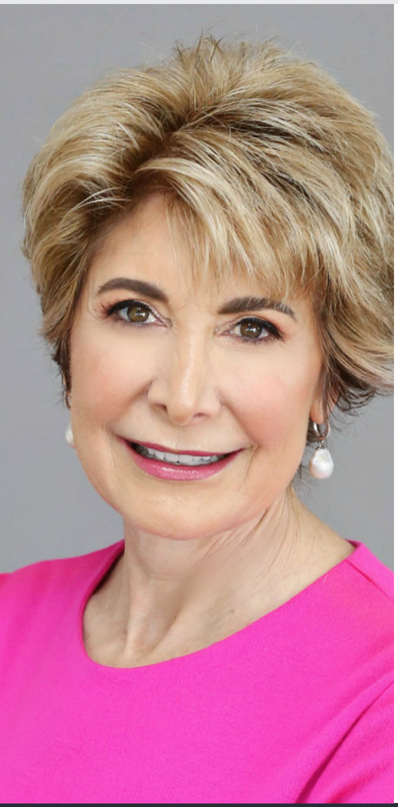
- State whether your organization has run tabletop exercises

Given the importance of cyber, I would suggest that boards begin these five key steps right away.

To learn more about these important topics, join me for a special briefing on March 28, 2023, at 11am EST, led by Google Cloud CISO Phil Venables, and featuring panelists Kevin Mandia (CEO, Mandiant) and Brian Stafford (CEO, Diligent).

To get the latest insights and trends shaping governance, risk, compliance and ESG, subscribe to the Diligent newsletter.

SUBSCRIBE NOW



About the Author

Betsy Atkins is a former three-time CEO and has served on some of the world's most visible global public company boards. For 30 years, she has worked behind the scenes at companies like Chico's, Vonage, Darden Restaurants, NASDAQ, HealthSouth, Wix and Home Depot Supply. She has served on over 30 boards and been through 13 IPOs, and she has served on many private equity- and venture capital-backed private boards. Betsy started her career as an entrepreneur, co-founding several successful digital tech and consumer companies, including blockbuster $5.4 billion Ascend Communications. She currently serves on the boards of Wynn Resorts, Volvo Cars and Diligent Corporation. Betsy is the author of the book *Be Board Ready: The Secrets to Landing a Board Seat and Being a Great Director*, and she is a regular contributor to WSJ, the Financial Times, Forbes, CNBC PowerLunch, Bloomberg and Yahoo! Finance.

About Diligent

Diligent is the global leader in modern governance, providing SaaS solutions across governance, risk, compliance, audit and ESG. Serving more than 1 million users from over 25,000 customers around the world, we empower transformational leaders with software, insights and confidence to drive greater impact and lead with purpose. Learn more at diligent.com.

For more information or to request a demo:

Email: info@diligent.com | Visit: diligent.com