Comments from Rod Hackman on proposed SEC Rule issued on March 9, 2022, regarding Cybersecurity Risk Management, Governance, and Disclosure

Introduction:

The opinions expressed in these comments are my personal views and do not reflect the opinions of any entity I am affiliated with.

I have led the cybersecurity oversight function for the past six years for an SEC registrant. The proposed SEC rulemaking is a major step in the right direction to address the gap in governance, disclosure, and oversight for cybersecurity. My views are informed by the attached document "Closing the Cybersecurity Governance Gap". This gap results from the combination of a lack of will, culture and knowledge at the board level and the challenge many CISO's face in communicating cybersecurity issues to the board and senior management. The unfortunate result is too often a "check-the-box" superficial approach to cybersecurity governance at the board level.

Comment #1: Definition of and Criteria for "cybersecurity expertise":

My concern relates to the proposed Item 407(j) which addresses "cybersecurity expertise". While I agree that a strict definition is unwise, I believe that the "non-exclusive list" is too narrowly focused on cybersecurity thereby inviting boards to adopt another "check-the-box" remedy by adding a CISO-type to their ranks and relegating all matters "cybersecurity" to that individual. Cybersecurity expertise possessed by CISOs is surely a necessary component, but alone is insufficient to properly deal with systemic contextual issues related to cybersecurity. For example, some CISOs primarily deal with compliance issues related to various regulatory requirements such as NIST, ISO, GDPR, etc. but do not possess a broader understanding of cybersecurity governance. Compliance is essential for the enterprise but is only a subset of cybersecurity governance.

Cybersecurity is one component of enterprise risk management (ERM). Cyber risk is a form of systemic risk. Therefore, cybersecurity governance requires at least a high-level understanding of complex systems. SEC registrants operate complex business enterprises which face major persistent systemic risk. Below is an excerpt from NISTIR 8286 which describes the complexity of major enterprise systems.

Excerpt from NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management
Paragraph 2.2.4 Increasing System and Ecosystem Complexity

Many systems upon which agencies and other institutions rely are complex, adaptive "systems- of-systems" composed of thousands of interdependent components and myriad channels. The systems operate in a rapidly changing socio-political-technological environment that presents threats from individuals and groups with shifting alliances, attitudes, and agendas.

The constant introduction of new technologies has changed and complicated cyberspace. Wireless connections, big data, cloud computing, and IoT present new complexities and concomitant vulnerabilities. Information and technology no longer represent the simple, automated filing

system. Rather, they are like the central nervous system—a delicately balanced and intricate part of any organization or enterprise that coordinates and controls the most fundamental assets of most organizations. This ecosystem's increasing complexity gives rise to systemic risks and exploitable vulnerabilities that, once triggered, can have a runaway effect with multiple, severe consequences for enterprises and the Nation. Managing cybersecurity risk for these ecosystems is incredibly challenging because of their dynamic complexity.

This complexity increases risk to specific systems and that risk can cascade to create additional risk at the system, organization, and enterprise levels. Moreover, emerging risk conditions created by the interdependence of systems and counterparty risk must also be identified, tracked, and managed.

My recommendation is to expand the "non-exclusive list" in Item 407(j) to include in the boardroom individuals with a contextual understanding of the interworking of complex systems, i.e., those with experience in operating or designing complex systems.

Comment #2: Definition of Cybersecurity

I suggest defining "cybersecurity" without using the word in the definition. Below are definitions provided by NIST and CISA.

NIST.SP.800: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cybersecurity & Infrastructure Security Agency (CISA): Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

ATTACHMENT

CLOSING THE CYBERSECURITY GOVERNANCE GAP

1. **It seems we hear about cyber-attacks daily. What is the Board's role in dealing with this problem?**

   Answer: *Yes, we are constantly being bombarded with cybersecurity problems to the point where Boards are becoming desensitized to breaches unless they directly affect their company or industry sector. This is a massive problem in both the private and public sectors. The Boardroom must actively engage in oversight to deal with it. However, moving the needle on Board oversight and governance solutions remains elusive. Boards ask questions but are challenged to put cyber-risk in the context of the infrastructure and risk controls in place for the enterprise they oversee. Boards need to understand the problem before they can govern it. The days of relegating this to the IT organization are over.*

2. **These attacks are pervasive, complex and seem to be overwhelming. How does the Boardroom begin to deal with them?**

   Answer: *Some companies, particularly those in the financial services industry, are dealing with cybersecurity effectively. However, many others are not. There have been numerous wake-up calls for more effective Boardroom oversight: SolarWinds, Colonial Pipeline and Microsoft Exchange, to name a few. In the case of SolarWinds, a derivative lawsuit has been filed against its directors. Board members understand this is a major issue but, given its size and complexity, they often struggle to find a roadmap to guide them in delivering effective governance and oversight.*

3. **So, what needs to happen to change that paradigm?**

   Answer: *To start with, Boards must accept and embrace cybersecurity oversight as a business issue requiring the attention of the entire Board. It is much more than an IT issue. The second step is for Boards to become more engaged and to continually resist a "check the box" approach to cybersecurity oversight, which is all too tempting given the size and complexity of the issue. Ask questions. Demand that the company's cybersecurity management professionals (generically referred to as "CISOs") and outside experts explain cybersecurity threats, processes, and procedures in plain language, not technical jargon.*

4. **Assuming Boards are eager to engage and tackle cybersecurity, how do you recommend proceeding?**

Answer: *I recommend a two-pronged approach: top-down and bottoms-up. The top-down approach starts with educating Boards, the C-Suite and CISOs to think about their "enterprises as systems" (EAS). A system is a regularly interacting or interdependent group of elements comprising the enterprise. Only by understanding how the EAS works and mapping out the interactions of system components can enterprise cyber-risk be fully understood and managed. A high-level assessment of the EAS also puts a boundary around these complex problems, helps the Board understand the business issues, and enables the Boardroom and the C-Suite/CSIOs to better communicate with one another. The results will be a contextual proactive approach rather than reactive approach to systemic cyber-risk. Without an understanding of the EAS, cyber-risk vulnerabilities cannot be put into context. With an understanding, design flaws, threat vectors and weak interfaces can be dealt with effectively: Other benefits ensue.*

Engage management and outside advisors to map the EAS. Be aware that mapping and understanding the EAS is an ongoing and dynamic process. Be prepared to both routinely reevaluate the EAS and to reevaluate it in anticipation of, and BEFORE major changes are made to the enterprise, either internal or external, such as digital transformation, new technologies, introduction of new subsystems, changes in third-party interfaces, acquisitions, divestitures etc. Too often, changes to the EAS caused by pursuing new business opportunities are made without considering their impact on enterprise-wide cyber-risk. Another element of the top-down approach is to adopt a cyber-risk management framework for the enterprise. There are several frameworks to choose from, such as NIST, ISO, SOC2, etc. The best framework is likely to be formed by selecting the best elements from each. To start this process, I recommend the NIST framework https://www.nist.gov/cyberframework . Why: 1) The concepts and processes are logical, intuitive, and easy to understand; 2) As you peel back the layers, the NIST framework offers excellent detailed procedures on how to deal with cyber-risk within the context of overall enterprise risk management (ERM) (See NISTIR 8286 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf); and 3) Draft congressional legislation mandates NIST as the basis for prospective guidance forthcoming from the SEC.

The bottoms-up approach begins with elevating the CISO and Internal Audit to present at the Board level and involving them in any changes to the EAS. This direct communications link is essential. Many companies employ good practices to mitigate cyber-risk, but Boards need to know if these protections are too much or too little? Does the Board understand them from a business perspective? Is the EAS resilient? Are the most important assets and processes of the EAS being protected? Does the company need to do more? This is the world of risk assessment, vulnerability testing, tabletop exercises, etc., and threats such as ransomware, cloud, supply chain, platform, insider, and so on.

How should the multitude of cyber-risks be dealt with? This depends on the magnitude of their potential impact on the company and their likelihood of occurrence. Risks can be dealt with in four ways. They can be avoided, accepted with mitigation, transferred to a third party

through insurance or ignored if minor. Cyber-risk management is different for each company depending on the complexity and nature of its business. Cyber-risk will never be zero. Balancing risk/reward will always be an ongoing challenge. Boards need to assess cyber-risk within the context of the company's operations and strategy. The result will be the development of both a risk appetite and tolerance which optimizes cyber-risk mitigation within budget constraints and minimizes the impact on the strategy and operation of the enterprise. Although seemingly overwhelming, cybersecurity can be understood within a business context at both the Board and C-Suite/CISO level. Effective Board governance starts with active Board engagement with the C-Suite/CISO. Active engagement will help the C-Suite/CISO understand cyber-risk from the Board's perspective and help the Board understand cyber-risk from the C-Suite/CISO perspective.

As the top-down and bottom-up approaches develop and mature, they should merge to create optimal Board/Management engagement and enhanced cybersecurity for the enterprise.

5. **Are Boards and committees properly organized to deliver effective cybersecurity oversight?**

***Answer**: While some are, many are not. Too often cybersecurity is dealt within the Audit committee, one which is already burdened with accounting and financial issues. Some companies stand up Risk committees. I think the best solution is a combined Tech & Risk committee which would be tasked with evaluating any changes to the EAS. The "Tech" function would evaluate the upside opportunity afforded by new business initiatives, while the "Risk" function would evaluate the potential downside and disruption to the EAS. However, a separate committee does not relieve the Board's responsibility to remain actively engaged in cyber-risk oversight.*

In addition, I predict fundamental changes in the culture of today's Boards will be a result of ever-increasing demands related to cybersecurity. Boards will have to work harder to get this right. At the same time, they are facing increasing liability as insurance companies charge more and cover less when it comes to the transference of cyber-risk. The combination of more work and more risk will cause some Board members to rethink their roles, particularly in publicly traded companies. Just as Sarbanes Oxley made increased demands on companies, and in particular their Audit committees, cyber-risk oversight (a much more complex job) will require more. It would be prudent for Boards to make changes today rather than wait for government regulators or market forces to dictate outcomes and put companies on the defensive.

6. **You mentioned government regulators. How do you see government involvement in risk oversight?**

   ***Answer**: Just as we have witnessed a dramatic increase in the number and seriousness of cyber incidents over the past few years, we have seen ever increasing involvement from government and regulators, from the White House on down, as they attempt to fix the problem. Whether it be through executive orders, legislation, or regulations, we can expect government involvement to accelerate. There is draft legislation requiring enhanced risk disclosure, cyber experts on boards and increased SEC scrutiny. Expect more! As regulatory intervention evolves, I expect legislators to mandate cybersecurity standards and dictate "SOX like" requirements for cybersecurity, despite the fact the cyber-risk oversight is a much more complex problem than finance and accounting. My prediction is that these requirements will be based on the NIST framework and procedures.*

7. **What is your closing message to the Boardroom?**

   ***Answer:** Cyber-risk is a business risk with the potential to negatively impact the value of your franchise due to a loss of operating capability and a loss of confidence by critical constituents. The demands made on Boards for systemic cyber-risk oversight are increasing at an alarming rate with no end in sight. Yes, let's face it, implementing and managing cyber-risk is the massively complex problem it seems to be. BUT, with the help of management and outside advisors, proactive Boards can and must understand and deal with this as the major business risk it is and apply the same judgement and oversight it applies to all other challenges and changes to their businesses.*