Blue Lava Response to Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

File Number S7-09-22

MAY 8, 2022

BLUELAVA

MANAGING THE BUSINESS OF SECURITY

May 8, 2022

Vanessa A. Countryman
Secretary, Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

File Number S7-09-22
rule-comment@sec.gov

Dear Secretary Countryman,

We are writing in response to the Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, and to express our broad support for it.

As background, Blue Lava is a security program management company built with, by and for the cybersecurity community. The company was founded on the premise of the increasing alignment of security programs to the business.

Cybersecurity program management is a critical capability for any organization - so it can measure, manage, and communicate the effectiveness of their program. Enabling executives to speak in the language of the business about their cybersecurity program management with confidence and ease is essential in today's digital world.

We consider having cybersecurity policies and procedures foundational to an organization - like breathing. And without proper governance, policies and procedures are useless when no one is accountable for their enforcement. A cybersecurity program must include other facets of the organization - just like you would any other business function:

- Operations
- Support
- Strategy
- Necessary funding (based on industry, size of company, and geography)

This is why a deep level of visibility into a holistic cybersecurity program is a critical function of building, supporting, and reporting on a cybersecurity program.

Our experience provides an important and essential perspective for responding to your request for feedback proposing policy changes that can advance the cybersecurity industry.

We have listed our responses below. We are available to meet and discuss our responses in greater detail, and are willing to support and engage with you and the broader cybersecurity community to ensure the proposed rule has the intended positive effects.

Very Best Regards,
David Walter
CEO, Blue Lava
david@bluelava.io

What follows is our responses to the questions you posed which we felt most comfortable answering.

17. Should we adopt Item 106(b) and (c) as proposed? Are there other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed under Item 106, to the extent that a registrant has any policies and procedures or governance? Conversely, should we exclude any of the proposed Item 106 disclosure requirements?

- We feel that 106(b) and (c) should be adopted in order to ensure that organizations have the right governance, oversight, and supporting cybersecurity investments with respect to people, process, and technology.
- However, providing more consistent and informative disclosure regarding an organization's cybersecurity risk management and strategies is going to be challenging for a few reasons:
    - First, the industry has been focusing on compliance frameworks, not cybersecurity program management. Compliance and cybersecurity are not the same thing, and a cybersecurity-centric framework and methodology that is continuously updated and managed throughout the year (not a point in time) would yield much more tangible and consistent insights.
    - Secondly, the current reporting at the Board level is usually through the lens of potentially outdated frameworks, which may be missing some key elements necessary to a holistic view of a cybersecurity program - specifically: Fraud, Account Takeover, Cloud Security, and Application Security.
- We recommend adopting a common language to support the ability to communicate or report on cybersecurity efforts consistently. A cybersecurity-centric holistic framework would help address that. It would need to reflect modern cybersecurity practices and domains, create simple and common language that can be applied across industries and understood by both technical and non-technical executives, and be flexible enough to adapt to shifts in technology and the threat landscape.

18. Are the proposed definitions of the terms "cybersecurity incident," "cybersecurity threat," and "information systems," in Item 106(a) appropriate or should they be revised? Are there other terms used in the proposed amendments that we should define?

- We feel that these definitions are adequate and no other terms need to be defined.

19. The proposed rule does not define "cybersecurity." We could define the term to mean, for example: "any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat." Would defining "cybersecurity" in proposed Item 106(a) be helpful? Why or why not? If defining this term would be helpful, is the definition provided above appropriate, or is there another definition that would better define "cybersecurity"?

- Yes, defining cybersecurity will be extremely helpful because currently the term is used loosely and has many different meanings or interpretations. We require a common definition.

- The proposal for the definition of 'cybersecurity', uses the word 'cybersecurity' in the definition multiple times. Please consider:
    - Any action, step, or measure to detect, prevent, deter, mitigate, or address any threat or incident of an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

20. Should we require the registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal function or through an external third-party service provider? Would such a disclosure be useful for investors?

- We believe that requiring the registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal function or through an external third-party service provider should be included. However, there are potential issues with public disclosure. For example - listing providers could mean that the provider becomes a target.
- We believe forcing transparency here would enable the market to develop a perspective on credibility and efficacy based on how often they're seeing a certain provider, and whether certain providers tend to often be associated with breaches. It could also make it more acceptable for companies to specify specific vendors associated with their breaches if they're already disclosing who they work with for solutions.

21. As proposed, a registrant that has not established any cybersecurity policies or procedures would not have to explicitly state that this is the case. If applicable, should a registrant have to explicitly state that it has not established any cybersecurity policies and procedures?

- Yes, any public entity should state whether they have or do not have:
    - Policies
    - Standards
    - A cybersecurity program that measures, manages, and communicates effectiveness
- The state of their cybersecurity program
- The governance of a cybersecurity program must be visible and reported to Executive Staff team members and the Board of Directors.
- The governance of a cybersecurity program must include an appointed executive or senior personnel responsible for cybersecurity.
- Policies, standards, and a cybersecurity program are useless if no one is accountable for their enforcement.

32. Should 407(j) disclosure of board expertise be required in an annual report and proxy or information statement, as proposed?

- We believe the disclosure of a person with cybersecurity experience that works with the Board should be required. It is our opinion that it will be difficult to have a trained and qualified

cybersecurity expert on every public Board. An alternative approach is to ensure th Board has access to a cybersecurity expert to work directly with the Board.

41. What are the economic effects of the proposed cybersecurity incident and cybersecurity risk management, strategy, and governance disclosures? Would those disclosures provide informational benefits to investors? Would registrants benefit from a potential decrease in cost of capital because of the enhanced disclosure? Are there any other benefits, costs, and indirect effects of the proposed disclosure that we should also consider?

- Disclosures will sharpen corporate focus on proactively improving their cybersecurity risk management, strategy and governance, therefore reducing business risk and expected loss exposures. These strong cybersecurity program management investments will increase shareholder value in the long-term because they will be aligned and measured against business objectives. As organizations work through digital transformation and adopting emerging technologies, cybersecurity will become an enabler to the business. Organizations must shift away from having the basics in their cybersecurity program to a holistic program that aligns to the business.

43. Would both types of the proposed disclosure, cybersecurity incident disclosure and cybersecurity risk management, strategy, and governance disclosure, increase the vulnerability of registrants to cybersecurity incidents? Would this effect be mitigated by any of the other effects of the proposal, including indirect effects such as registrants' potential strengthening of cybersecurity risk management measures? What would be the impact of the proposed disclosure on the likelihood of future incidents for registrants? Would that impact be the same for both types of disclosure?

- Public disclosure in any form would certainly make a company a further target. Consider requiring companies to perform certain functions - potentially securing and closing any related gaps before disclosing. This approach could allow for the required time it may take to identify and address an issue and will influence organizations to increase the effectiveness of their cybersecurity program.

44. Would the proposed incident disclosure increase registrants' compliance costs to fulfill the proposed disclosure requirements related to incident reporting? What would be the magnitude of those costs? Would the proposed cybersecurity risk management, strategy, and governance disclosure lead to indirect costs such as hiring a board member or staff to their management team with cybersecurity expertise, or costs to devise, implement or improve the processes and procedures related to cybersecurity?

- There will be incremental costs associated with new disclosure and compliance requirements; however history has proven time and time again that the subsequent reductions in expected loss exposure(s) greatly outweigh the costs of those investments. It is our belief and experience that the benefits greatly outweigh the costs. That is the fundamental tenet and value of risk

management and public transparency - a company's cybersecurity program will become more effective and efficient.

46. Are there any specific data points that would be valuable for assessing the economic effects of the proposed cybersecurity incident and risk management, strategy, and governance that we should consider in the baseline analysis or the analysis of the economic effects? If so, please provide that data.

- Reports and analysis such as the Verizon Data Breach and Investigation Report (DBIR) provide good insights into the nature and impacts of cybersecurity incidents, and can be used to quantify the frequency and impact of cybersecurity risks.

49. Would any of the proposed amendments have disproportionate costs for smaller reporting companies? Do smaller reporting companies face a different set of cybersecurity risks than other companies?

- Yes, it is likely that the costs of complying with these new rules will be higher for smaller companies relative to their overall budgets. It is one of the reasons why the larger a company gets, the more it is able to invest in its cybersecurity and risk management programs. This can be potentially offset however by the use of effective and affordable cybersecurity program management tools, cybersecurity risk management tools and common approaches to reporting on cybersecurity.
- The risk exposure for smaller companies is generally smaller, given expected loss exposures correlate with the revenues at risk, volume of customer records, etc. However the risks themselves would be similar.

50. Are there any other alternative approaches to improve disclosure of material cybersecurity incidents, cybersecurity risk management, strategy, or governance that we should consider? If so, what are they and what would be the associated costs or benefits of these alternative approaches?"

- The industry has historically been focusing on compliance frameworks, not cybersecurity program management. Compliance and cybersecurity are not the same thing. A cybersecurity-centric framework and methodology would yield much more tangible and consistent insights.
- The current reporting at the Board level is usually through the lens of an industry framework, which is missing some elements necessary to a holistic view of a cybersecurity program - specifically: Fraud, Account Takeover, Cloud Security, and Application Security.
- Finally, there is no common language or taxonomy to support the ability to communicate or report on cybersecurity efforts consistently. A cybersecurity-centric framework would help address that.