From:	Nelson Novaes Neto
To:	cyberframework
Subject:	CSF 2.0 - Draft: Feedback and Recommendations - Govern Pillar
Date:	Thursday, September 14, 2023 1:23:13 PM

Hello Members of the Cybersecurity Framework,

I am Nelson Novaes Neto, a MIT Research at Cybersecurity at MIT SLOAN.
We are very happy that NIST has included a new pillar, Govern, into the Cybersecurity Framework. This is a very important pillar, and we are glad that NIST has recognized its importance.

We believe that our research paper, "7 Pressing Cybersecurity Questions Boards Need to Ask," (https://hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask) which was published in the Harvard Business Review, is totally aligned with the Govern pillar. We would like to contribute to the development of this new version of the Cybersecurity Framework, and we believe that our paper can help to improve the Govern pillar and bring more details and important topics for this new pillar. Related with the Govern and senior leadership responsibilities, we recommend adding more explicit directions for Board Members and executives leaderships:

The board of directors has fiduciary and oversight responsibility for the organization's cybersecurity posture. This means that the board is responsible for ensuring that the organization has a strong cybersecurity program in place to protect its assets and operations. The board should have a clear understanding of the organization's cybersecurity risks and should set and enforce cybersecurity policies and procedures that are designed to mitigate those risks. The board should also ensure that cybersecurity is integrated into all aspects of the organization's operations and that cybersecurity risks are considered in all decision-making processes. The board should also communicate effectively about cybersecurity with the organization's stakeholders. This includes communicating the organization's cybersecurity risks, policies, and procedures to all employees, customers, and partners. The board should also regularly review and update the organization's cybersecurity program to ensure that it is effective in protecting the organization from cyberattacks.

The board's fiduciary and oversight responsibility for cybersecurity is important because cyberattacks can have a significant financial and reputational impact on organizations. By taking steps to mitigate cybersecurity risks, the board can help to protect the organization's assets and operations and ensure its long-term success.

Board Member responsibilities:

- The board of directors should have a clear understanding of the organization's cybersecurity risks. This includes understanding the threats and vulnerabilities that the organization faces, as well as the potential impact of a cyberattack.
- The board of directors should set and enforce cybersecurity policies and procedures. These policies and procedures should be aligned with the organization's risk appetite and should be designed to protect the organization's assets.
- The board of directors should ensure that cybersecurity is integrated into all aspects of the organization's operations. This includes ensuring that cybersecurity is a top priority for all employees and that cybersecurity risks are considered in all decision-making processes.

- The board of directors should communicate effectively about cybersecurity with the organization's stakeholders. This includes communicating the organization's cybersecurity risks, policies, and procedures to all employees, customers, and partners.
- The board of directors should regularly review and update the organization's cybersecurity program. This is important to ensure that the program is effective in protecting the organization from cyberattacks.

The board should also understand and know how to answer each of the 7 questions that are posed in the research paper, "7 Pressing Cybersecurity Questions Boards Need to Ask." These questions are:

1. What are our most important assets and how are we protecting them?
2. What are the layers of protection we have put in place?
3. How do we know if we’ve been breached? How do we detect a breach?
4. What are our response plans in the event of an incident?
5. What is the board’s role in the event of an incident?
6. What are our business recovery plans in the event of a cyber incident?
7. Is our cybersecurity investment enough?

Please, let me know how we can contribute more with this new pillar and the importance of the board of directors.

Thank you
Nelson Novaes Neto