From: Shilpa Sawant
Sent: Friday, November 3, 2023 11:22 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Feedback || Discussion draft of NIST Cyber Security Framework 2.0

Dear NIST CST2.0 team,

RE: Discussion draft of NIST Cyber Security Framework 2.0
Dated : 3rd Nov 2023

Thank you for providing us an opportunity to submit feedback and comments on the revised framework.

I appreciate the efforts made by NIST in developing the Cybersecurity Framework 2.0 draft and its commitment to addressing current and future cybersecurity challenges for organizations across the globe. I have been an advocate of NIST CSF and have been using it extensively. I have aligned it across every new program that I have designed.

I would like to provide a few inputs after reviewing the draft. My feedback is as follows :

1. Section 2.1 : Including " Govern" in the CSF scheme of things makes the CSF holistic and complete. In the depiction in Fig 2. Framework Functions, GOVERN is in the center of the wheel because it informs how an organization will implement the other five Functions. However, In my view Govern should be placed in the outermost circle and inner circle should cover Identify, Protect, Detect, Respond and Recover as Govern should have control and oversight for the other 5 functions to perform effectively. In this draft, it depicts as if 5 functions are handling the Govern function.

2. Section 3.1.1. : Ways to use profiles.
Another point could be added where Profiles can be used to perform a due diligence assessment before acquisition and set a target profile to be achieved on Legal Day 1 of acquisition.While it might get covered in the Risk Management programs, expressing it explicitly would result into heavy adoption of this framework.

3. Appendix C : Framework Core - Inputs on the sub-categories

Govern:
1. GV.RR : In order to address the Cyber Security skills gap and also improving cybersecurity competency within the organization, Competency & SKills for Workforce development to be put in place, should be added as another sub category.

2. GV.PO.02 : Introduce Legal and regulatory compliance as one of the requirements. Sample statement is as follows.

E.g., Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission and applicable legal and regulatory compliance requirements

3. GV.OV : Include another sub-category on Establishing Governance committees for having adequate oversight on a timely basis.

Identify:

ID.RA.01 : Introduce Risk V=based Vulnerability management concept.

E.g., It could be reframed as : Vulnerabilities in assets are identified, validated, and recorded (formerly ID.RA-01, PR.IP-12, DE.CM-08) and a risk based approach is taken to remediate them.

ID.RA.09 : The authenticity and integrity of hardware and software are assessed prior to acquisition and use. This appears as a one-time assessment. Considering the rise in supply chain risks, regular assessments are required to stay aware of the risks.

E.g., The authenticity and integrity of hardware and software are assessed prior to acquisition and use and also, assess them periodically to minimize the risk

ID.IM.02 : Include terms such as drills, stress testing exercises as they are very relevant for cyber resiliency.

E.g., Security tests, drills, stress testing exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements

Protect:

PR.AA.02 : Suggesting to incorporate Risk based authentication or 2nd factor authentication. Alternatively, Strong mechanisms for Identity validation to be put in place. This will help in enhancing the security maturity across the organization.

PR.AT.03 : New Sub-category on reinforcing awareness on a regular basis to be included for completeness. As of today, one time awareness is merely a tick in the box for employees. It should be reinforced regularly to make it a habit to follow cyber security practices.

PR.DS : Suggest to embed a sub category on identification of sensitive data, accordingly CIA of data in rest and transit can be protected. It will be an overkill for any organization to protect all the data.

PR.IR-01: Networks and environments are protected from unauthorized logical access and usage. Would it be possible to include proper network segmentation to restrict or limit the compromise statement.

Detect:

Adverse Event Analysis (DE.AE <https://urldefense.com/v3/__http://de.ae/__;!!Nhox7I4E!MKynyFMqsNRbqFlz8d9SOuErxDEGwzreFN72NG3hXFxwQ7mApP9111X2adON20ZLHDl5hlZ5zegmESMg820-pr_GRA$ >): Threat hunting action to identify threats proactively to be a part of threat detection. to be considered to be included and DE.AE.09

The approach of Respond and Recover are very specific to staying proactive. However, In this era, where Cyber attacks or breaches are inevitable, emphasis could be made around strong recovery technologies, testing of contingency plans and points related to post-incident recovery procedures could be included.

Request you to go through my views and incorporate them in case they are valid and relevant for today. These recommendations are my personal opinions and are not on behalf of any organization.

The feedback was primarily for the enhancement of the framework to ensure it is relevant and effective in the coming years ahead.

Thank you for your consideration.

Regards,
Shilpa Sawant
Cyber Security Practitioner
NIST CSF Follower
Shilpa Sawant