From: Carlota Sage
To: cyberframework
Subject: Feedback on the NIST CSF 2.0 Public Draft
Date: Friday, November 3, 2023 4:05:51 AM

As someone who has worked in Enterprise IT organizations, as a community evangelist for a security vendor, as a consultant to major organizations, and who now serves as a virtual CISO for sub-500 employee organizations, I feel the NIST CSF 2.0 draft doesn't give enough weight to the importance of culture and awareness in securing an organization, no matter how small or large that organization is.

I suggest making Culture and Awareness its own category under governance. Example below.

Category: Security Culture & Awareness (GV.CA)
"Organizational leadership is responsible for and accountable for fostering a culture that is risk-aware, ethical, and continually improving."

Subcategory
GV.CA-01: Regular Security Awareness Training is provided to the organization's employees and contractors as a whole, with additional training provided to high risk departments and individuals.

Ex 1: General security awareness training is provided on a regular (yearly, quarterly, or more often) basis.
Ex 2: Software developers and IT personnel are allotted an individual training budget which may be used towards conference attendance.
Ex 3: Marketing and Sales teams are given additional training securing devices prior to trade shows.

Subcategory 2:
GV.CA-02: Leaders provide a shared understanding of ethical expectations and provide appropriate guidance.

Ex 1: Leadership implements an ethical training program and documents examples of ethical behavior they expect to see modeled in the organization.

Subcategory 3:
GV.CA-02: Community engagement is prioritized as a security measure.

Ex 1: Leadership provides a central community or communication space where non-security personnel can safely ask questions and get resources in protecting themselves both inside of and outside of the organization.
Ex 2: Leadership identifies champions in non-security organizations that the security team can engage to test messaging and incident response, and to be trusted voices within their unit.

Thank you for your consideration.

--
Carlota Sage
Founder & Community CISO

[redacted]

Pocket CISO, LLC
[redacted]