From:	Bob Galley
To:	cyberframework
Subject:	NIST CSF 2.0 - Idea for Awareness and Training controls (PR.AT)
Date:	Monday, August 14, 2023 11:28:28 PM

Source: Roger Grimes' commentary on the new CSF within his LinedIn newsletter. (1) NIST Updates Their Cybersecurity Framework for Good and Bad | LinkedIn

Roger had mentioned how the new PR.AT section consolidates its controls to two: One for all users, and another for privileged access users. Both use a very generalized phrasing, and Roger listed several points that he'd like to see in the framework. Essentially, to consider the source of most attacks (social engineering still makes up 90% of initial attempts), to include testing, and to make sure that awareness isn't one-time but ongoing.

From that, I had the below idea.

The way the new framework is structured, would it be possible to define what the "awareness and training" skills are? Like a PR.AT-0? They could future-proof it by saying, "Training should proportionately focus on current prevailing access methods per (other named standard) and include trending new methods that apply to the company. Training should, be ongoing / cyclical and should include both a theory and a practical application (testing) component."

The new phrasing looks very much like my old company's highest-level security policy. "We will establish a SETA program." The current "The awareness and training will give employees the skills to perform their tasks with a security focus" is really vague. Granted, it allows for a lot of different methodologies, but I think we can give the definitions some shape and still allow for freedom of how to apply it.

Respectfully,
Bob Galley, CISSP