From: Matthew Rosenquist
To: cyberframework
Subject: NIST CSF v2 FEEDBACK
Date: Friday, October 13, 2023 11:16:38 PM

In the interest of time, I will keep my feedback brief and only focus on the most important issue.

The most significant weakness of the current model is its lack of focus on understanding the intelligent adversaries. It remains predominately an inward-looking framework, which imposes significant limits on overall effectiveness.

Think of it this way – imagine you were the coach of a professional football/futbol team and were playing for the championship. NIST CSF would be fine at understanding your strengths and weaknesses, of individual players and maybe even defensive and offensive lines. It would even be applicable at evaluating the condition of the field. But that is only half the picture a great coach would seek. Perhaps even more importantly is the piece which is missing – an understanding of the opposing team. What are their strengths, weaknesses, resources, typical plays, and behaviors? This is half of the challenge of any complex adversarial engagement! Sun Tsu spoke of both knowing yourself AND your enemy. The same holds true today in cybersecurity.

If you want to provide a significant increase in the value of the CSF model, add a PREDICTION group with subgroups that look at threat agents, threat method intelligence, evolutionary practices, tying into early attack sensors beyond your network, understanding the capabilities of Threat Agent archetypes, and extrapolating where future attacks are likely. This is real and significant value.

Great famously stated "He who defends everything, defends nothing.".

Take this opportunity to upgrade to deliver significant value, and not just calling out a layer that was already integrated into how organizations were already operating.

Matthew Rosenquist,

CISO, Cybersecurity Strategist, and Industry Advisor
(34 years of experience and a reputation that showcases innovation and evangelism)