Comment Submission to the NIST Preliminary Cybersecurity Framework
December 10, 2013

Submitted by: Garcia Cyber Partners
Comment type: General

Comment Summary

The descriptions of the Framework Implementation Tiers on pages 9-11 include an assessment of "External Participation" at all tier levels, yet there is only vague reference, and no formal mapping, to "external participation" among the Framework Core Categories and Subcategories in Appendix A, pages 13-26. Thus, the Implementation Tiers have n anchor or guidance to assess "External Participation" capability maturity among the Core Categories.

Comment Discussion

Many enterprises manage formal "stakeholder and partner engagement" or "partnership and collaboration" programs. They assign executive teams to develop and manage a structured system to coordinate external engagement, information sharing and best practices exchange with internal operations and coherent risk-management planning. These programs are designed to synthesize all the relevant but diffuse input from employees' external engagement efforts that otherwise may not be effectively sorted, prioritized and operationalized to benefit the company's risk management strategy.

Put another way, effective management of these programs can leverage and, when appropriate, align with lessons learned, best practices and threat intelligence that can only accrue from a collective attention to cybersecurity challenges and interdependencies that are common across the critical infrastructure community. It can be argued that this external engagement function is a necessary component (or "Category") across all of the five Core functions of Identify, Protect, Detect, Respond and Recover. This is so because there is generally-accepted view that, to succeed against the many complex cyber security threat and vulnerability challenges, an enterprise should not rely solely on its own strategies, tactics and situational awareness in isolation of stakeholders in the broader ecosystem, including sectoral partners, suppliers, customers, law enforcement, intelligence agencies and others.

There are references in the Core that touch on this concept at the margins, but they are neither explicit nor pervasive across the Core as they should be. These are in the "Business Environment" and "Governance" Categories under the "Identify" Function, and the "Communications" Category under the "Respond" and "Recover" Functions.

It may be that there are no specific Informative References that outline the disciplines and skill sets necessary to carry out such an external participation program, and thus that could be identified as a gap for future resolution.

Suggested Change

Include in each of the Core Functions a new Category called "External Participation" that includes subcategories and descriptions of external participation activities that support the Core Function and that can be measured for alignment with the Implementation Tier descriptions. One example of this suggestion is provided for the "Identify" function on the next page.

Small to mid-sized enterprises with limited resources will not realistically be able to support all elements of a cybersecurity external participation program, but that dynamic should nevertheless be reflected in the Framework as a real-world capability gap between large and small enterprises, in a way that suggests potential new services or business models to fill those gaps.

Email: greg@GarciaCyberPartners.com **Phone: 443-510-8641**

EXAMPLE OF A NEW CATEGORY ("EXTERNAL PARTICIPATION") WITHIN THE FIVE CORE FUNCTIONS

Function

IDENTIFY (ID)

Category

External Participation (EP)

The system and management of coordinated activities and processes among key organizational personnel for engaging with external partners and stakeholders to develop collective situational awareness and community of trust to identify threats, vulnerabilities, and best practices that inform, and can be operationalized to improve, an effective cybersecurity risk management strategy.

Sub-Category

ID.EP-1: A identified executive or team whose sole function is the management and coordination of an external partnership program across the organization's enterprise functions and lines of business

ID.EP-2: Enterprise membership in the relevant industry sector coordinating council(s) and information sharing and analysis center(s), or other relevant sectoral or cross-sectoral collaboratives engaged in critical infrastructure protection activities under the Identify Core Function

ID.EP-3: Involvement as appropriate in government partnership programs intended to assist, and learn from, the private sector o matters related to identifying real-time and developing critical infrastructure threats and vulnerabilities, and best practices for mitigation.

ID.EP-4: External engagement program for international cybersecurity initiatives

ID.EP-5 Involvement in or cognizance of joint industry/academic research or conferences aimed at identifying and understanding the evolving threat environment

Informative References

-
-
-

** This example offers only an illustrative list of activities for one Core Function, and thus can be considered a basis for further discussion about this and the other Functions.

Email: greg@GarciaCyberPartners.com **Phone: 443-510-8641**