From: **Sounil Yu**
Date: Mon, Apr 10, 2017 at 2:33 AM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: cyberframework@nist.gov

NIST,

I'm providing feedback here as a private citizen and not on behalf of my organization.

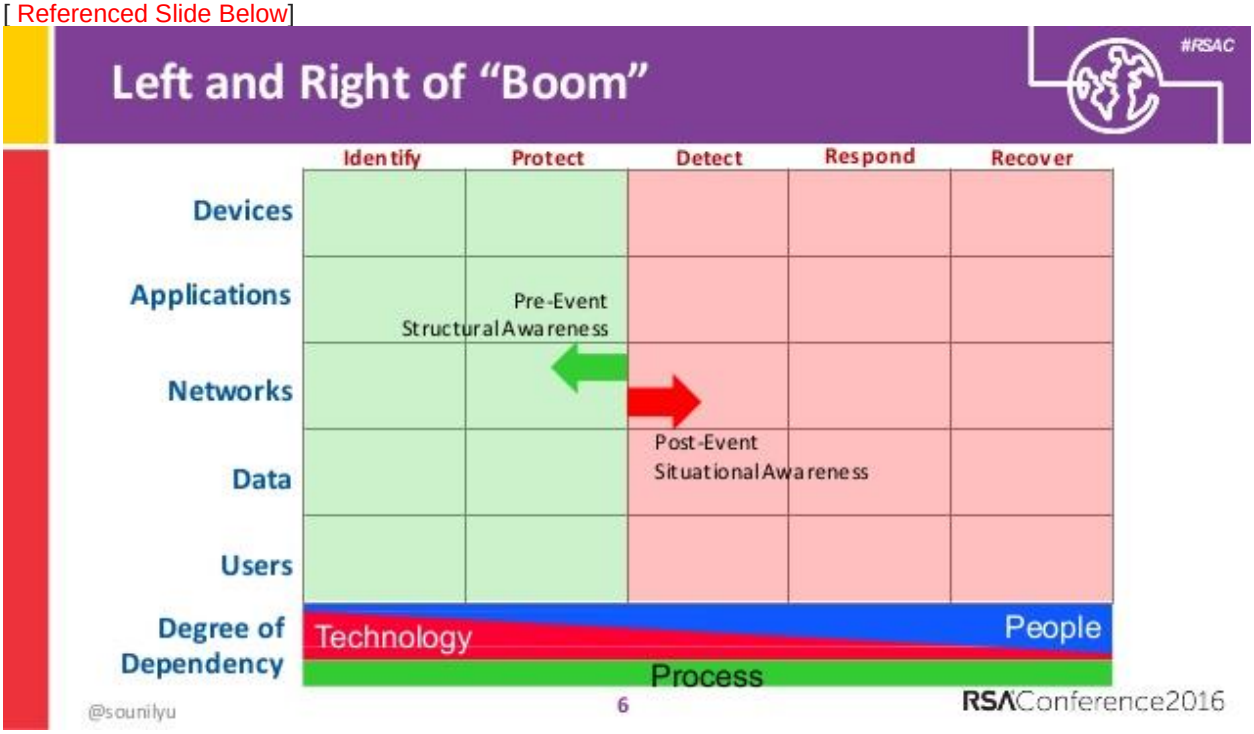
My comments are based on my work on the Cyber Defense Matrix, which incorporates the CSF as a core element. You can find details about the Cyber Defense Matrix at:

https://www.slideshare.net/sounilyu/understanding-the-security-vendor-landscape-using-the-cyber-defense-matrix-60562115

From my study of the Cyber Defense Matrix, I have come across a few discrepancies within the Framework:

1. **IDENTIFY vs DETECT**. To explain this discrepancy, I need to establish some common terminology and constructs. Let's presume that "BOOM" happens between PROTECT and DETECT. (See slide 6 in my slides). BOOM can be any event or alert that was observed/monitored/logged.

[Referenced Slide Below]



LEFT of BOOM, we need STRUCTURAL awareness
RIGHT of BOOM, we need SITUATIONAL awareness

Structural awareness includes many activities from the IDENTIFY function: Knowing an asset exists (inventory), knowing how important it is to me (prioritization/impact), knowing its attack surface (vulnerabilities)

Based on our structural awareness that an asset exists, that it is sufficiently important to me, and that there exists an attack surface (i.e., a vulnerability), one makes a risk management decision to determine whether to move to PROTECT. What moves you from PROTECT to DETECT is a BOOM event. The BOOM may be entirely innocuous or completely devastating. The purpose of DETECT is to obtain SITUATIONAL awareness to look at and analyze the events that transpire and determine if there is a need to RESPOND.

With these basic concepts and definitions, a discrepancy emerges with respect to where we put “vulnerabilities":

Do we IDENTIFY vulnerabilities (e.g., ID.RA-1) or do we DETECT vulnerabilities (e.g., DE.CM-8)?

Webster's defines vulnerability as being "open to attack or damage”. Understanding one’s vulnerabilities gives awareness around one’s attack surfaces and structural weaknesses. Thus, vulnerability scanning (DE.CM-8) should be captured in IDENTIFY, not DETECT. The DE.CM description/action to “verify the effectiveness of protective measures” should also be moved somewhere under IDENTIFY. (Also, to avoid confusing IDENTIFY and DETECT further, I suggest avoiding the term “IDENTIFY” anywhere in the descriptions associated with DETECT. For example, Security Continuous Monitoring [DE.CM]: The information system and assets are monitored at discrete intervals to {validate | analyze | detect } cybersecurity events.)

2. **COMPLETENESS OF COVERAGE ACROSS ALL ASSET CATEGORIES**. To explain this discrepancy, I have to refer again to my matrix, where I explicitly call out the asset categories of DEVICES, APPLICATIONS, NETWORKS, DATA, and USERS. In a couple cases, the Framework covers these categories inconsistently. For example, in Asset Management (ID.AM), specifically in the context of inventorying, only three of these asset categories are covered (ID.AM.1-**Devices**, ID.AM.2-**Applications**, ID.AM.3-**Networks**). ID.AM.5 touches upon DATA, but only in the context of prioritization. Furthermore, ID.AM.5 doesn’t cover prioritization of USERS and there’s no “inventorying” of USERS. This inventory and prioritization of USERS is independent from the defining of cybersecurity roles in ID.AM.6. To further highlight the inconsistency, looking at PROTECT, one can think of Awareness and Training (PR.AT) as “patching” or “hardening” the USER. Since we have USERS covered in the PROTECT function, it would seem reasonable to naturally include USERS in the IDENTIFY function as well.

Likewise, in the case with DETECT, we have four of the categories covered (DE.CM.2/DE.CM.7-**Devices**, DE.CM.4/DE.CM.5/DE.CM.7-**Applications**, DE.CM.1-**Networks**, DE.CM.3/DE.CM.7-**Users**). Any discussion of DETECT in the DATA category is missing despite ample coverage of the DATA category in PROTECT (PR.DS).

———————

There are other dimensions to the Cyber Defense Matrix, which enable us to cover gaps in the original CSF (e.g., Supply chain security, which has been addressed in v1.1) as well as other issues that haven’t been adequately addressed in v1.1 (e.g., data privacy, fraud, etc.)

This v1.1 document is a small incremental change and so it should remain in the v1.x series. A v2.0 should warrant a much more substantial update. For such an update, I would recommend incorporating the additional dimensions represented in the Cyber Defense Matrix as these additional dimensions do not complicate the Framework but rather add more structure and context that actually helps simplify our understanding of the cybersecurity space. These additions would provide a sufficient level of change to promote the Framework from v1.x to v2.0.

Regards
Sounil Yu