Feedback on Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

From: Mauricio Tavares [redacted], Privacy Test Drivers

General:

- Just the tables listed make this document be more than 20 pages long. As I asked during the workshop, who is the audicence for this framework? If we hope small and medium business (SMB) will adopt this (some of them are defense/critical infrastructure contractors), we should ask ourselves if the framework is too complex for a 1-10 person business. While this is not SP800-171 complex, it has enough subcategories to lose the audience unless there is a way to tie them down and show the flow.

Sometimes that can be done by just mentioning on the text which (sub)category should be followed after a give subcategory is completed (see below), but I think a diagram/flow chart of just the categories and how they related to each other would help tremendously the more visual members of the crowd, yours truly included. Start with Table 1 and use the same colours for consistency sake, but then indicate which categories go to which ones (at certain points, some steps will be take in parallel).

- Sometimes a given category may/should refer to another one. Since this is PDF file, make that reference a link. I consider this extremely important as it would help to follow the flow of events between each category; I added a few examples of references to related categories in the examples starting on page 23 (see below)

p.4.

ID.RA-01: Current examples seem to be first party only. For a third party, we could take, say, example 4 and create

"3rd party provides the first party information regarding the results or current status of their vunerability testing. First party, also provides to the 3rd party any findings obtained from its own vulnerability testing if they can help 3rd party patch or improve its software."

i.e. it should be a two-way road.

PR.PS-02: Change the "and" in

"Software is patched, updated, replaced, AND removed commensurate with risk"

to "or"

"Software is patched, updated, replaced, OR removed commensurate with risk"

Also, Example 1.5: "Plan for out-of-schedule emergency patches."

p.23-26

In the following examples, I broke a single example into multiple steps so they can show the progression of events. Note I did not add examples for all the steps; if there is more time I can do so.

RS.MA-01:

Example: "Users report sluggish website. Initial investigation indicates an increase in activites reported by the logs, and recommend the event to be classified as possible cybersecurity incident, which triggers the incident response plan."

RS.MA-02:

Example: "Per incident response plan guidelines, the original event is determined to be a true cybersecurity incident: a website attack."

RS.MA-03:

Example: "According to the incident response plan, a website attack is a priority cybersecurity incident. SME for the website are contacted."

RS.MA-04:

Example: "Further monitoring indicates the attack may possibly accessed the the database serving website. Priority has increased to high and more experts are added. Incident response manager is contacted (RS.CO)."

RS.MI-01:

Example: "Decision is made to cut the website connection to the external word so data cannot be taken. Management agrees and website is down."

RS.MI-02:

Example: "vulnerability that was exploited is identified and patched (PR.PS-02)"

RS.MA-05:

Example: "Indicent response plan recommends to contain incident (RS.MI) and start recovery (RC.RP)"

RC.RP-02:

Example: "Experts determine the extent of the damage to the database, and how much can be saved (changes from last backup to now)."

RC.RP-03:

Example: "Database backup is tested for integrity. Data that was changed since last backup that can be saved is collected."

RC.RP-04:

Example: "Database is restored from backup. Transactional data that was saved since last backup is added."

RS.CO-01: If this is dropped, the subsequent categories need to be renumbered.