From: Thomas Schneider
To: cyberframework
Subject: Comments about the NIST CSF Core v2.0 draft
Date: Friday, August 25, 2023 12:52:23 PM

NIST CSF team,

Thank you for soliciting feedback. There are many changes in NIST CSF v2.0 Core that I think are valuable improvements. One of these would be the addition of the Govern function and the Categories and Subcategories under it that emphasize the importance of governance and oversight. The overall reorganization of v2.0 clarifies the framework. For example, moving many of the categories/subcategories in v1.1 Identify into Govern. Similarly, moving the somewhat unrelated subcategories that had been in Information Protection Processes and Procedures (PR.IP) in v1.1 into more specific categories in v2.0 adds clarity to the framework.

I think the added emphasis on risk management, and especially enterprise risk management is a beneficial enhancement. These Subcategories, in my opinion, align closely with concepts in COSO ERM and ISO 31000, and it would be good if they remain in the final revision of v2.0 as is or with minimal changes:

> GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood
> GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
> GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies

The addition of “Enterprise Risk Management” to GV.RM-03 is helpful because ID.GV-4 in v1.1 did not explicitly call out the use of ERM as a tool for managing cybersecurity risk. Hopefully “Enterprise Risk Management” will remain in GV.RM-03 in the final version of 2.0.

Regarding third-party risk management, I think Subcategory GV.SC-04 (“Suppliers are known and prioritized by criticality”) is a good addition. In my experience many organizations do not prioritize suppliers, and therefore do not provide sufficient oversight to their most critical vendors.

For Asset Management, I like that ID.AM-05 emphasizes the need to prioritize assets, and how ID.AM-07 calls out the need for **“**Inventories of data and corresponding metadata” as a distinct subcategory rather than bundling data inventory in with other asset inventories.

For Roles and Responsibilities, I think that consolidating ID.AM-06 and ID.GV-02 from v1.1 into one Subcategory, GV.RR-02 in v2.0 is a good change as ID.AM-06 and ID.GV-02 seemed to be redundant. I also think that adding “authorities” to GV.RR-02 is important because it implies that for someone to be responsible, they need to be given the authority to execute their responsibilities.

I also like ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use as the replacement for “PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.” PR.DS-8 seemed to imply something like ID.RA-09, but ID.RA-09 is more

straightforward and is easier to understand.

There are also a few subcategories in v2.0, that I think should be reconsidered before v2.0 is finalized:

Regarding the new Subcategory PR.DS-10: "The confidentiality, integrity, and availability of data-in-use are protected'" which was formerly PR.DS-5: "Protections against data leaks are implemented," to me these subcategories do not apply to the same locations for data. I think of data in use as it is described in Wikipedia, "**Data**[1] **in use** is an information technology term referring to active data which is stored in a non-persistent digital state typically in computer random-access memory (RAM), CPU caches, or CPU registers." As I interpret them, PR.DS-5 in v1.1 is more closely related to data loss prevention (which might include data at rest in a non-approved location such as a personal workstation, or data in transit being transmitted to a non-approved location) as opposed to data-in-use. While the addition of PR.DS-10 to cover data-in-use provides coverage that may have been missing in v1.1, I think that "Protections against data leaks" or text like it, should remain in the CSF, possibly as an additional subcategory.

Regarding Incident Response and related plans, I miss the specificity of v1.1 PR.IP-9: "Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed," which has been replaced by ID.IM-04: "Cybersecurity plans that affect operations are communicated, maintained, and improved." Would NIST consider reinserting the parenthesized text, i.e., "(Incident Response and Business Continuity)" from PR.IP-9 into ID.IM-04? I assume that the intention of this change was to make the Subcategory apply to additional plans beyond Incident Response and Business Continuity, however, lack of an Incident Response plan seems to be a prevalent enough issue at organizations that I think it would be useful to call it out specifically.

For the same reason, I would recommend re-adding "Response and recovery plans" to the v2.0 Subcategory ID.IM-02. Again, I think that many organizations do not perform incident response testing even if they have an IR Plan. So, in my opinion it would be helpful to specifically cite a test of the IR Plan in ID.IM-02, or call out the need for a test of the IR Plan in some other subcategory. While ID.IM-02 with its present wording should apply to an IR Test, some organizations may not interpret it that way unless the subcategory specifically lists it. Also, NIST may want to reconsider the order of the subcategories in ID.IM. As they are now, the tests for the plans in ID.IM-02, come before the subcategory, ID.IM-04, that appears to be the one that requires the plans to be created.

Thanks, and I hope that you find these comments useful.

Regards,

Tom Schneider