Comments on the NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Introduction

On February 2022, NIST announced an RFI for evaluating and improving NIST cybersecurity resources[i], particularly the CSF v1.1. Back then, I had to chance to comment[ii] on the RFI and provide various recommendations and insights.

One year afterward, and after reading the concept paper[iii] and attending the two CSF v2.0 journey workshops I was glad to see some of my ideas and those of the community considered. I would like to take this opportunity further to comment on the paper and highlight some of the topics that I see worth addressing in the coming release of CSF v2.0.

1. Updating the Framework Roadmap

The last roadmap[iv] was laid out by NIST about 4 years ago (April 2019). It would be interesting if NIST kept refreshing the roadmap (e.g., on yearly basis) to reflect current framework discussions and potential areas for improvement in future releases. This will help align the efforts and put all the stakeholders in the picture while going forward.

In the same context, it would be interesting if NIST fixes a consistent timeframe (e.g., 3 to 5 years) for regular framework review and enhancement.

2. Aligning with business objectives

It would be interesting to specify the intended audience for the document, what is expected from them, and what they can benefit from the framework to help put things into context.

In addition, presenting the contribution of the framework to create and preserve the business value should be considered in the document. Furthermore, alignment and linkage between cybersecurity and business-related objectives and strategy should be also discussed.

In addition, and as an optional framework, it would be interesting if use cases be added to the document to help convince management to invest in cybersecurity while preserving its value.

In this regard, ISACA did a great job in COBIT 2019 within their framework introduction and methodology document[v] laying out the business case for implementing a governance and management system (see Making the Case) and linking governance and management objectives back to stakeholder needs and drivers (see Goal Cascade).

3. Addressing the human element

Humans are the weakest link in cyberspace. Verizon, for instance, in their latest data breach investigation report[vi] stated that 82% of breaches involved the human element.

While the framework listed numerous practices for managing cyber in various levels and areas, few practices address people. ISO did great in their latest revision of ISO 27002 by adding a whole new category to lay out people-related controls. Just to name a few, human factors such as behavior, culture, ethics, errors, resistance to change, and social engineering attacks … could be considered for inclusion.

4. Addressing compliance and assurance issues

It would be interesting if the role of the framework can be presented to demonstrate due care and diligence. Ideas regarding how the framework can be used for compliance and assurance activities can be shared within the document.

In the same context, NIST can also consider adding new subcategories for ensuring internal control, auditing, assurance-related activities, and outcomes.

5. Enhancing incident handling activities

NIST may consider providing more guidance on incident response planning, testing, and execution. For the same, ISO recently updated the incident management series of standards (ISO 27035-1, 2, 3, and 4-draft) and can be used as a reference for the same.

6. Providing operational guidance

Great to see the formwork remains technology- and vendor-neutral, however, it would be interesting to mention various operational capabilities that can be leveraged to better manage cyber risk. Such effort will also help security service and product providers to map the features of their offerings to the framework listed operational capabilities.

7. Classifying activities and outcomes

NIST did a great job by introducing the control baselines (low, moderate, and high impact) into their publications. The same thing can be seen in the CIS critical security controls with their implementation groups (IG1, IG2, and IG3).

It would be interesting to see similar ideas in CSF 2.0 to help businesses prioritize cyber-related activities and outcomes based on their context and the criticality of their assets.

8. Clarifying categories and subcategories

To simplify the task for readers, it would be wise to rename categories and subcategories using clearer terms such as outcomes or practices. In addition, adding a new column to describe subcategories would be beneficial to define the intent behind them, explain the activities and the intended outcomes.

9. Identifying control names and titles

Besides just listing control numbers (e.g., A.15.1.1, A.15.1.2, A.15.1.3) within the informative references, it would be extremely handy to include also control names and/or titles to make life easy for practitioners and make sense of those controls and the purpose behind them.

10. Listing training resources

To help spread the knowledge It would be great to list within the NIST framework website the variety of education and training resources that can be used to learn more about the framework, and to gain additional knowledge and practical skills regarding its implementation.

Regards,

Bachir Benyammi

[i] https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

[ii] https://www.nist.gov/system/files/documents/2022/04/26/04-25-2022-Bachir_Benyammi_Redacted.pdf

[iii] https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

[iv] https://www.nist.gov/document/csf-roadmap-11-final-042519pdf

[v] https://www.isaca.org/resources/cobit

[vi] https://www.verizon.com/business/resources/reports/dbir/