Monday, April 24, 2023

Nozomi Networks Feedback to the January 2023 "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework"

Nozomi Networks commends the National Institute of Science and Technology (NIST) for its continued efforts to equip global industries with consistent and coherent guidance and reference material for cybersecurity activities, goals, and risk management priorities. The Cybersecurity Framework represents a pillar in the cybersecurity community, and it is incredibly important to underscore the broad applicability and utility of the CSF to date.

As a global solution provider of industrial cybersecurity products, we have witnessed robust implementation of the NIST CSF since our founding in 2013, with national and international customers widely adopting the Frameworks' Categories and Subcategories to outline and guide risk management programs.

Working primarily with owners and operators with a wide array of industrial control systems and operational technologies, we see a vital role to identify, protect, detect, respond, and recover from cyber incidents based on deep understanding of legacy technology and asset inventories, vulnerability mapping and management, threat intelligence and detection, and broader situational awareness and anomaly detection for data rich, information poor environments.

Despite the common language that the Framework delivers across industries and sectors, each company or organization still must identify internal teams or champions who act as their own independent advisors, having to do literature reviews and consensus mapping cross-referencing relevant standards, regulations, suggestions, and best practices. Security leaders and teams must map, prioritize, and deconflict:

- The status of their security program, risk ownership, and visibility gaps
- Existing management and mitigation tools, resources, and capacity
- The development environment of third-party products and security management of suppliers
- Enterprise content management, data security and PII
- Operational products and services, hardware, software, IoT, cloud offerings, etc.
- Upstream and downstream supply chain
- Operational technology and cyber-physical security
- The sea of available add-on security products

With this in mind, below are several responses to the questions outlined in the Concept Paper.

1. **Do the proposed changes reflect the current cybersecurity landscape (standards, risks, and technologies)?**

The proposed changes in the Concept Paper reflect consistent and coherent expertise across a wide range of standards, risks, and technologies. Potential additional thoughts and components to consider in the CSF 2.0 revision:

- How can the Framework and the new emphasis on both cybersecurity governance and supply chain risk management work to identify and remediate single points of failure across operations or sectors? For example, from reliance on cloud computing, similar technologies and suppliers, inputs from separate sectors, etc.
    - Borrowing from the April 2021 joint NIST and CISA white paper "Defending Against Software Supply Chain Attacks" the CSF 2.0 could also provide similar steps for building resilience and considering alternative plans and operations.
        - "1. Pre-identify and establish alternative suppliers for the critical software you use
            - Have plans in place to switch to a new supplier, if feasible, when critical software becomes unavailable or presents an increased risk
        - 2. Use your understanding of how software supports critical business or mission functions to identify failover processes and workarounds in the event functionality with specific software becomes unavailable
            - Prepare written failover processes for critical software
            - Periodically conduct table-top exercises or walk-throughs to ensure your organization understands the steps in its failover processes
            - Where possible, coordinate failover processes with vendors and other external stakeholders"
- Where else might the CSF 2.0 point to and incorporate the April 2021 joint NIST and CISA white paper "Defending Against Software Supply Chain Attacks"?
- How important is continuous monitoring for entities and organizations? (mentioned nearly 40 times in the NIST SP 800-82r3 "Guide to Operational Technology (OT) Security, but only 3 times in the 2018 CSF)?

2. **Are the proposed changes sufficient and appropriate? Are there other elements that should be considered under each area?**

With an OT/ICS perspective, though understanding the broad applicability of CSF, please consider inclusion or discussion of the following:

- How specific security controls impact an organization's risk tolerance – this may be appropriately captured or demonstrated in the developed CSF Profiles or CSF Profile template resources
    - This may be extremely important and unique for OT environments, where tolerance understanding and calculations are typically different from IT and depend widely on the type of operation, the vendor components at risk,

accessibility, and the associated downtime and downstream effects of remediation.

- When developing metrics for advancing the understanding of cybersecurity measurement and assessment, the CSF 2.0 could consider metrics that lead entities and organizations to self-evaluate their implementation of the CSF in two categories:
    - Preparedness**:** by assessing means-based prevention capacity – an organization's maturity in implementing the CSF that is demonstrably effective against known risks and TTPs. E.g., detection and remediation of vulnerabilities is a metric.
    - Resilience: by assessing effects-based prevention capacity – an organizations ability to prevent worst case effects by cyber means, regardless of known risks and TTPs. E.g., an alternative asset or manual process is established for any at risk crown jewel asset.

3. **Do the proposed changes support different use cases in various sectors, types, and sizes of organizations (and with varied capabilities, resources, and technologies)?**

The proposed changes support various sectors, types, and sizes of organizations, assuming the OT applications are further supplemented by the NIST SP 800-82r3. The changes further support the enduring and flexible nature of the CSF to transcend risks, sectors, technologies, and national borders. Since the CISA Common Performance Goals are organized in line with the CSF Categories, it would be interesting to cross-reference the CISA CPGs especially in terms of maturity to the CSF 2.0 or potential methods for metrics and measurement.

- It may also be useful and informative to categorize or tier appropriate and available Informative References based on their maturity in relation to the CSF 2.0

When promoting Governance to its own function, the CSF 2.0 should encourage the separate urgency for OT cybersecurity governance, which is equally critical to managing and reducing cybersecurity risks. Where the CISA CPGs encourage a specific OT cybersecurity leader, the CSF 2.0 should outline where OT cybersecurity requires unique approaches to governance in terms of identifying and being responsible for OT specific cybersecurity risks, reporting, and the differences for remediation, containment, incident response, etc. and potential process downtime and cascading impacts.

4. **Are there additional changes not covered here that should be considered?**

When emphasizing incident response and preparedness, it is essential to consider the evolution of detection capabilities for cybersecurity. Intrusion detection, vulnerability detections, threat activity detections, and baseline network behavior anomaly detections from machine learning capabilities are different types of notifications to investigate. Some of these detections can make the difference between a cyber event mitigated in time, and a major cybersecurity incident responded to and recovered from. The Respond category lists "notifications from

detection systems are investigated." For the expansion of incident response mechanisms, it may also be worthwhile to further expand on categories within the Detect function: Anomalies and Events, Security Continuous Monitoring, and Detection Processes.