Security Bits, LLC **www.securitybits.co**
securitybits@securitybits.co

To whom it may concern,

Thank you for allowing us to participate in the discussions for the direction of the draft version of the National Institute of Technology's Cyber Security Framework Version 2. We believe this new version of the cybersecurity framework is a good increment from the previous version.

The addition of the Govern function to this iteration of the NIST CSF will assist organizations greatly in maturing their security posture within two key areas, first by bringing visibility and ownership of security into higher levels of the business and second by providing an enforcement and oversight component that can be used to drive metrics and demonstrate both the effectiveness of the overall security program as well as to outline key areas that need improvement. Incorporating Supply Chain Risk Management is another valuable addition to this version of the framework particularly as we move into more complex IT environments that span across disparate and global networks, adopt the use of third-party software and platforms, and diverse business relationships (e.g., partnerships, mergers, acquisitions).

Recommended Change Considerations

Metrics

The term "metrics" isn't specifically called out in any of the six core functions, but there are similar terms used throughout the draft framework that involve metrics collection (e.g., calculating, analysis, collected). We feel the term "metrics" would fit in the Govern function under GV.RM-06, in the Response function under RS.AN-03 and RS.AN-06, and somewhere in the Recover function to measure how effective an organization's cyber resilience is. Oversight of a cybersecurity metrics program fits best under the Govern function, but alternatively it could potentially fit under the ID.IM category. In our experience we've found that historical metrics collected and reported to the CISO leads to determining how effective the people, processes, and technology are performing over time which can then drive strategic initiatives and budgets effectively addressing improvements across the six functions within the NIST CSF framework.

Secure Baseline Configurations

There is no specific mention of secure baseline practices (e.g., disabling default accounts, shared credentials, or unused services). Although this is more technical and varies from organization based on operational needs, a broad statement could be used such as "define software and application baseline standards that provide only the necessary requirements for the operation of the assets and the functional roles of operators". This fits best under PR.PS, but PR.AA does partially cover this using the term "least privileged". Additionally, a footnote reference to NIST SP 800-207 would be useful.

Detection and Response Measurement

Measuring throughout the detection and response activities enables organizations to understand their effectiveness and make adjustments with the security strategy. The Detect function does call out the recommendation to monitor, but the term “measure” isn’t used specifically. It would be ideal to include the term “measure” to advise organizations that both the comprehensive collection of the data and the subsequent analysis move the security posture towards an improved security program maturity. Some examples of these measurement metrics could be Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), “Break Out Time”, and Time to Recovery (TTR). Those metrics combined with resource expenditures for incident detection and response can provide security leaders a clear picture of the cost per incident and gaps involving people, processes, or technologies. This recommendation fits best under the RS.CO and/or DE.AE categories.

Conclusion

The biggest challenges we have seen with organizations who haven’t matured their cybersecurity programs are:

(1) Insufficient monitoring/visibility
(2) Lack of metrics collection, reporting, and evaluation of that data to address deficiencies
(3) Reactive instead of being proactive (e.g., Threat hunting, Incident Response/Resilience Plan Testing, Purple Teaming, Detection Engineering, or Cyber Threat Intelligence)
(4) Security is not built into the technology on-boarding process (i.e., Secure system baseline configurations before operation and policies to use least privilege/zero trust models)
(5) Incomplete understanding of the attack surface and assets across the organization – “we can’t secure what we aren’t aware of” (e.g., Shadow IT, BYOD, Cloud Services, Remote Workforce)

We feel a significant portion of this new framework drives most of these challenges we have observed and the content will assist organizations to improve their cybersecurity maturity. We appreciate the opportunity to contribute to the draft of NIST CSF Version 2 and look forward to the final release.

Brandon Newton
Chief Security Officer, Security Bits