1. Introduction

Veritas Technologies would like to thank NIST for giving us the opportunity to comment on the discussion draft of their CSF 2.0 Core. It reflects NIST's commitment to fostering a collaborative environment where stakeholders from government, industry, and academia can contribute to the development of a framework that remains both relevant and effective.

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers (including 91% of the Fortune 100) rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware.

2. Comments

GOVERN (GV)

Veritas believes that CSF 2.0 should articulate that, in order for enterprises to understand where their exposure lies, they should classify and identify their data prior to any CSF event occurring. Veritas appreciates that Govern encompasses all the other aspects of CSF, but it should be a practice to have knowledge of their data to govern before the CSF event occurs.

One aspect of Govern that often gets overlooked (and may be outside the intent of this document) is the need to capture and potentially monitor content for the purpose of: (1) capturing public records for the U.S. National Archives and Records Administration (2) capturing communication to enable Freedom of Information Act responses (3) capturing communications for future investigations, litigation etc. In the past, email was sufficient. Today, communication happens in so many ways, it is essential to capture all channels or actively prevent use of non-standard communications by federal employees. This also helps to uncover insider threats through active monitoring & classification.

RECOVER (RC)

Veritas recommends changing "*Restore assets and operations that were impacted by a cybersecurity* 223 *incident.*" to "*Restore* ***and re-gain control over the*** *assets and operations that were impacted by a cybersecurity* 223 *incident."*

Veritas recommends that this additional information be added after the RECOVER (RC) bullet on Page 6: Veritas knows that data recovery can be a complex endeavor, needing knowledge of the organization's most critical assets. Recovery may hinge on the detailed understanding of tactics, techniques, and procedures (TTPs) required to meet recovery timelines as well as the technology, teams, and processes needed to restore those assets following an incident. Veritas recommends a discussion of this complexity, either here, or elsewhere in the Framework.

Figure 2 Framework Functions

Veritas questions whether this process is more linear, and even overlapping, rather than circular. Veritas recommends that NIST consider a linear graphic beginning with "IDENTIFY" in which "GOVERN" somehow covers each of the other components.

Appendix C. Framework Core: Table 4

Veritas believes the “RECOVER” function needs much more detailed build-out. Our 40 years focused on the backup-and-recovery function have yielded key insights into elements comprising a more robust RECOVERY capability.

Table 8: DETECT (DE)

Please add this as a subcategory under Continuous Monitoring (DE.CM) in Table 8 on Page 40: Veritas recommends that the backups are secure via scans of the backup images to provide the confidence for recovery from backups.

Table 10. RECOVER (RC)

Veritas would like to see the following additional elements in this section. Please add this list of subcategories under Incident Recovery Plan Execution (RC.RP) in Table 10 on Page 43:

a. Review of the Isolated Recovery Environment.
b. Scanning of immutable backups.
c. Prioritized recovery of mission-critical data, applications, and assets.
d. Effectively handling evidence, such as logs and images, that will aid law enforcement to recover stolen assets.
e. Standard Operating Procedures must include recovery of critical systems as a best practice as part of the Recovery phase. Some industries do this activity as a regulated entity, but this should be extended to all enterprises. Veritas feels that it should be done periodically to understand their recovery at scale but at least perform this for the most mission critical systems is a start.
f. As part of the recovery phase, Veritas would like to present the importance of recovering in an isolated environment and running through the latest malware scans prior to production deployment after an incident.

3. SUMMARY

NIST's release of the Cybersecurity Framework 2.0 draft invites stakeholders to provide their valuable input and insights. This updated framework represents an essential milestone in the ongoing effort to enhance the cybersecurity posture of organizations and individuals.

This collaborative effort holds the promise of fortifying the cybersecurity landscape and safeguarding critical infrastructures, economic assets, and personal information. By participating in this process, stakeholders can play a vital role in shaping the future of cybersecurity, making it more resilient and adaptive to the evolving threats of our interconnected world.