Rubrik Comments on NIST Cybersecurity Framework Version 2.0

Rubrik appreciates the opportunity to provide input on NIST's Cybersecurity Framework Version 2.0. Rubrik supports NIST's efforts and believes that the evolution and successful implementation of the Cybersecurity Framework will enhance the cybersecurity posture of all types of organizations. As explained in greater detail below, Rubrik believes that more focus on data security and cyber resiliency should be infused into the Cybersecurity Framework to ensure that organizations operate with an "assume breach" mindset and have a cyber recovery plan that ensures complete cyber resiliency.

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business and mission resilience against cyberattacks, malicious insiders, and operational disruptions.

The world's leading organizations rely on Rubrik to uphold data integrity, deliver data availability, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

Based on insights from helping organizations recover from various cyber-attacks successfully, we offer the following best practice recommendations:

Recommended Changes to NIST CSF Version 2.0 Subcategories:

- **GV.OC-05**: Add "data" to this category; proposed text:
  - **GV.OC-05**: Critical outcomes, capabilities, data, and services that the organization relies on are determined and communicated (formerly ID.BE-1 and ID.BE-4)
  - **Justification:** Rubrik believes that data is a critical dependency to every organization and every organization should identify what data is most critical for every outcome, capability and service.

- **ID.AM-07**: Add "to include approved, denied and expected locations"; proposed text:
  - **ID.AM-07:** Sensitive data and corresponding metadata (to include approved, denied, and expected locations) are inventoried and tracked

- **Justification:** Rubrik believes that metadata generated around the access or attempted access to data and where that data resides and the access requests occur provide rich context and should also be tracked.

- **PR.AA**: Add "to include SaaS applications and cloud storage"
  - **Identity Management, Authentication, and Access Control (PR.AA**): Access to physical and logical assets (to include SaaS applications and cloud storage) is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)
  - J**ustification:** Rubrik wants to ensure that SaaS applications and cloud storage be referenced to ensure the readers understand the importance in those areas.

- **PR.PS-04**: Add a recommended retention timeframe for logs
  - **PR.PS-04:** Log records are generated for continuous monitoring and should be retained for a minimum period of time (e.g. 30 days) (formerly PR.PT-1)
  - **Justification:** A minimum amount of time should be recommended for log retention to better ensure that organizations can rapidly triage and recover from various types of events.

- **PR.IR-03:** Immutability should be added as a mechanism for infrastructure resiliency
  - **PR.IR-03: Mechanisms (e.g., failsafe, immutability, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-5)**
  - **Justification:** Cyber threat actors are aggressively targeting data backups to obtain the upper hand in ransom and extortion negotiations. Immutable backups are the bare minimum for any organization to realistically believe their data will survive a cyber-attack.

<u>Recommended Additions to NIST CSF Version 2.0 Subcategories:</u>

- **GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored using several techniques such as Software Bill of Materials (SBOM) and Supply Chain Level Software Artifacts (SLSA) over the course of the relationship (formerly ID.SC-02, ID.SC-04)**

    - **Justification:** Rubrik asserts that in light of the escalating frequency of supply chain attacks, exemplified by incidents such as SolarWinds, log4j, and Progress MoveIT, it is essential to meticulously maintain an inventory of software components and rigorously verify their authenticity and integrity.

- **ID.RA-10: Identifying, analyzing, assessing, evaluating, prioritizing, monitoring and managing information security risks generating from the usage / adoption of emerging technologies such as Generative Artificial Intelligence, Industrial Control Systems, Operational Technology, Drones, etc.**
    - **Justification:** Rubrik recognizes that as technologies swiftly evolve and industries progress on their digital transformation paths, the embrace of emergent technologies like Generative AI, ICS/OT, Drones, and others will play a pivotal role in the Industry 4.0 revolution. However, this advancement also broadens the threat landscape. It not only amplifies the risks at the software asset level but extends them to the hardware asset tier as well. Consequently, it becomes imperative to emphasize the importance of a robust security risk management program tailored for these emerging technologies.

- **ID.RA-11: Data leaving an organization to be utilized by trusted third parties and partners is identified, recorded, and audited**
    - **Justification:** It is critical for organizations to have a full understanding and record of what data leaves their environment (authorize and unauthorized).

- **PR.AA-07: Access to cloud hosting and SaaS applications administration are identified, monitored, and audited**
    - **Justification:** As organizations migrate and expand the adoption of SaaS applications and cloud-hosted workloads the impacts of events are much greater. Having visibility and records of administrative functions is crucial to ensure and minimize the impact of rogue users and cyber threats.

- **PR.DS-12: Organizations should have Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for their data and systems.**
    - **Justification:** RTO is the maximum amount of time an organization can return to normal operations after an outage or data loss. RPO is the organization’s goal for how much data the organization can tolerate losing.

- **PR.DS-13: Backups are kept according to industry standards, including immutable copies**
    - **Justification:** Cyber threat actors are aggressively targeting data backups to obtain the upper hand in ransom and extortion negotiations. Air-gapped, immutable, access-controlled backups are the bare minimum for any organization to confidently and rapidly recover from a cyber-attack.

- **PR.PS-07: Firmware is patched, updated, monitored, and removed commensurate with risk**
    - **Justification:** Raising awareness and criticality to ensure Firmware is secured is critical as it will help reduce a major attack vector.

- **PR.IR-05: Immutable Backups are leveraged to protect critical data through a cyber-attack and leveraged during faster triage of attacks**
    - **Justification:** In incident response engagements, organizations are reluctant to install, query, and analyze production servers for fear of impact. It is more trustworthy, reliable, faster, and safer to conduct as much forensics analysis on data backups to quickly triage an attack and not tip off the cyber threat actors because they could trigger follow on attacks if they know the victim is on their presence.

- **PR.IR-06: Orchestrated recovery data actions are conducted, expanded, refined, and tested on a recurring basis**
    - **Justification:** Organizations should develop, plan and test their recovery actions and build automated recovery actions so that when incidents occur the path to recovery is expedited, tried and tested and validated without the pressures to figure this out during the stress of the incident. Being prepared reduces the chances that recovery steps won't be implemented incorrectly, out of sequence, or done so in a way that allows the threat actor(s) to come right back in.

- **DE.AE-09: Review of unexpected or anomalous/off-trend data access for known or new user or system accounts**
    - **Justification:** Continuous monitoring and trending of data access and patterns is a good way to identify and detect cyber threat actors early in the attack lifecycle.

- **DE.CM-010: Data backups are evaluated and monitored for adverse cybersecurity events**

- **Justification:** Cyber threat actors routinely target victim data backups in the early stages of their attack to corrupt, degrade or destroy them prior to acting. It is imperative for organizations to prioritize the security of their data backups.

- **RC.CO-05: Review all incident actions for improvements and needed areas. Implement a plan to mitigate all identified issues and make the organization more resilient. Track this after-action review in a formal, predictable manner with an annual review of all incident events over time.**
  - **Justification:** It is imperative that organizations fully understand the scale, scope, and root cause of incidents and are vigilant in their response and post-incident monitoring to ensure that they eradicated the threat(s)'s access and also know what data had its integrity and/or confidentiality degraded.