From: **Tony Urbanovich**
Date: Tue, Apr 4, 2017 at 6:01 PM
Subject: CyberGRX Comments to CSF draft v1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Kevin Ford, Missy Gillette

NIST:

CyberGRX is pleased to offer NIST the following feedback regarding the Draft NIST Cybersecurity Framework Version 1.1 based on its observations as a leader in the Supply Chain Risk Industry. Should you have any questions on our submission, please feel free to contact me or Missy Gillette directly.

Tony Urbanovich
Chief Operating Officer
CyberGRX
www.cybergrx.com

[Attachment Copied Below]

Comments to NIST on the NIST Cybersecurity Framework Draft v1.1

27 March, 2017

Table of Contents

Introduction

CyberGRX is pleased to offer NIST the following feedback regarding the Draft NIST Cybersecurity Framework Version 1.1 based on its observations as a leader in the Supply Chain Risk Industry.

Built by and with security practitioners, CyberGRX provides a comprehensive supply chain cyber risk management platform that addresses the existing inefficiencies of supply chain risk management. Through its innovative design, automation, and advanced analytics, the CyberGRX platform enables enterprises to cost-effectively and collaboratively identify, assess, mitigate, and monitor an enterprise's cyber risk exposure across its entire vendor, partner and customer ecosystem.

Framework Tiers

The third-party cyber risk management approach taken by companies today are typically manual, inefficient and not scalable to effectively address increasing cyber exposure. CEOs, business leaders, and risk and security managers need a better way to manage cyber risk in the expanding digital ecosystem of vendors, partners and customers. As such, CyberGRX commends the inclusion of third party risk management into the tiers.

CyberGRX offers the following comments regarding CSF v1.1's additions to the tiers:

- Tiers - Section 2.2: Our experience is that many organizations may only achieve a Tier 1 or 2 as regards SCRM but may be Tier 3 or 4 in all other regards. The disparity may spark conversation regarding splitting Tiers for Risk Management Process, Integrated Risk Management, Eternal Participation, and Cyber Supply Chain Risk Management (e.g. "Can we be a 3 in Integrated Risk Management and a 1 in SCRM?").
- Tiers – Lines 348 through 356: Terms are not clearly defined, intertwined and confusing to the reader. At this point in the document the concept of a "Framework Profile" and "Target Profile" have been introduced. However, there has been no discussion / definition of an "Assessed Profile". Additionally, the concept(s) of "Tier determination", "Tier selection", "Tier designation" and "assessed Tier" are not clear, nor the distinction between these concepts.
- Tiers - Line 352: Agree that Tier selection will naturally effect the Framework Profiles.
- Tiers - Line 353: Not sure what "risk disposition expressed in a desired tier" means. Agree that a tier will naturally affect the selection of a Target Profile. Not sure that risk, or a disposition of risk, is encapsulated by the Tiers.
- Tiers - Line 353: Suggest clarifying/replacing language "Similarly, the organizational state represented in an assessed Tier will indicate the likely findings of an assessed Profile, as well as inform realistic progress in addressing Profile gaps" with language that more clearly emphasizes relationship of business qualities in the tiers to activities and outcomes in the profiles" E.g. "An organization's activities regarding risk analysis and risk management, as described by the Tiers, will inform the prioritization of selections

within a Target Profile. It will also increase the fidelity at which the organization understands its security activities and outcomes based on assessment and monitoring."

- Tiers - Line 354: Agree that an organization's Tier will affect the findings of a Profile when assessed. Linking Profile and Tier Assessments is confusing. Linking Tier assessment and gap analysis is also confusing. Please clarify.
- Tiers - Line 381: Agree with language
- Tiers - Line 401: Agree with language
- Tiers - Line 427: Agree with language
- Tiers - Line 543: Unclear as to how Tiers express varying risk tolerances. Perhaps change to: "Varying risk tolerances will result in different tier selections."
- Tiers - Line 564: Add "desired" before "Implementation Tier". Change "should be" to "may be".

Supply Chain Risk Management

The interconnected nature of business strategy has expanded dramatically over the past few decades, from outsourcing of niche back-office components to an increasingly complex web of vendors, partners and customers that form a highly dynamic and globally distributed digital ecosystem.

As this interconnectivity grows, third and fourth party relationships are increasingly a source of cyber attacks, system failures, and data exposure that threaten an enterprise's ability to deliver products and services to their clients and customers; expose an enterprise to legal action, regulatory penalties and/or substantial remediation costs; and undermines customer confidence, damaging the enterprise brand.

CyberGRX offers the following comments regarding CSF v1.1's additions concerning supply chain risk management:

- Supply Chain - Section 2.2: Commend the inclusion of Cyber Supply Chain Risk Management in the Tiers. However, we recommend expanding the definition of Cyber Supply Chain Risk Management to be more inclusive. Something at the end of line 347 such as, "When considering the scope of Cyber Supply Chain Risk Management, organizations should consider an external service provider, supplier, vendor, external partnership, affiliate, and/or subsidiary who has access to company facilities, systems, and/or information and who provides a product or service."
- Supply Chain - Section 3.3: This discussion is good but it requires more information regarding partner security practices not related strictly to products. Services provided by partners, or data exchanges ancillary to procurement of products (i.e. financial records associated with product purchase) may contain critical information that must be secured. Therefore, more is required to secure the supply chain than products built to security specifications. Organizations not only require assurance that a product/service is safe, but also that the infrastructure and support associated with the product/service over its lifecycle are safe. In relation to the supply chain, organizations consider:

    - How secure are acquisition transactions?
    - How safe are my account details?
    - How safe are my partners maintenance services?
    - If the partner is attacked, will my operations/data be safe?
    - Could an attack on a partner create down time for our organization longer than our maximum tolerable down time?
    - Does the partner's risk appetite and risk tolerance match our organization?
- Organizations should also consider activities to continuously monitor the risk posed by supply chain partners to their digital ecosystem. This thought should be considered as another bullet in lines 610-617.
- Supply Chain - Line 370-372: Agree with Tier 1 SCRM Language.
- Supply Chain - Line 386-391: Agree with Tier 2 SCRM Language.
- Supply Chain - Line 409-417: Agree with Tier 3 SCRM Language.
- Supply Chain - Line 443-450: It has been our experience that the exchange of risk information between organizations is hampered by the number and variety of questionnaires/assessments/monitoring points. Large organizations can only assess the risk of a small percentage of partner relationships in any given year, while their suppliers have too many requests for risk information to address them all. Therefore, we commend the inclusion of formal means of requesting and receiving supply chain risk information. We further recommend that organizations and supply partners seek SCRM services that standardize and facilitate exchange of risk information between partner organizations to increase the bandwidth of communication between organizations and suppliers.
- Supply Chain - Line 587: Transition is jarring. Make SCRM its own subsection or rename 3.4 to Cyber Supply Chain Risk Management.
- Supply Chain - Line 602: Replace "manager" with "manage".
- Supply Chain - Line 609: Two periods in sentence – remove one.
- Supply Chain - Section 3.4: Agree with the use of target profiles in buying decisions
- Supply Chain - ID.SC-1: Can easily be incorporated into ID.RM-1. Including supply chain in ID.RM-1 suggests integration of SCRM into enterprise risk management.
- Supply Chain - ID.SC-2 - ID.SC-5: Agree with subcategory language but not sure that the subcategories belong in ID Function.
- Supply Chain - ID.SC-2 - ID.SC-5: These subcategories should be moved into existing subcategories in other functions.

Conclusion

CyberGRX has been pleased to leverage aspects of the Cybersecurity Framework in our efforts to mitigate supply chain risk. CyberGRX appreciates the opportunity to provide comments to further the development of the NIST Cybersecurity Framework and looks forward to working with NIST to address critical issues in supply chain risk management.

Questions regarding CyberGRX or this submission may be directed to the attention of Missy Gillette via email at missy.gillette@cybergrx.com.