From: **Orlie Yaniv**
Date: Mon, Apr 10, 2017 at 1:08 PM
Subject: Gigamon Comments to Draft Update 1.1 of the Cybersecurity Framework
To: cyberframework@nist.gov

Attached please find Gigamon's comments to draft version 1.1 of the *Framework For Improving Critical Infrastructure Cybersecurity.* If you have any questions or comments, please do hesitate to reach out to me directly at the email and phone numbers listed below.

Best regards,
Orlie Yaniv

--
Ms. Orlie Natalie Yaniv
Founder and Managing Member
Orlie Yaniv Strategies LLC

[Attachment Copied Below]

Gigamon appreciates the opportunity to provide comments to the draft version 1.1 of the *Framework for Improving Critical Infrastructure Cybersecurity* (Framework). Gigamon supports the efforts of the National Institute of Standard and Technology (NIST) to evolve and improve the Framework to enable organizations of all sizes to more effectively manage cybersecurity risk.

To that end, Gigamon recommends that NIST incorporate guidance that encourages organizations to view their cybersecurity activities at a systemic level, and evaluate whether the system enables cohesive and optimized implementations of the Framework functions, categories, and subcategories to provide the desired level of risk management in the most cost effective manner. By coordinating cybersecurity activities so that they function cohesively on an ongoing basis, organizations will be able to achieve an effective implementation of their risk management strategy.

In addition, Gigamon recommends that NIST expand the roadmap to include application of the Framework to network environments that lack traditional perimeters and don't utilize firewalls as a primary mechanism to manage risk. With the rapid adoption of cloud and mobile technologies and the advent of the Internet of Things and an explosion of devices and data, security becomes exceeding difficult. NIST should consider future security models where organizations rely on risk management at the user, device, and data/data classification/data communication levels rather than the existing network-based paradigm.

In support, Gigamon offers the following detailed edits:

Executive Summary

- Add the following sentences to line 106 after the sentence endingwith the phrase 'each dollar spent':

  Organizations may achieve effective cybersecurity resource allocation by evaluating their risk management strategy at a systemic level to ensure that their cybersecurity activities function together cohesively and with optimal effectiveness. A systemic approach will ensure that organizational risk management strategies align with both critical business objectives and resource limitations.

2.1 Framework Core

- Replace the existing paragraph describing Identify at lines 300 to305 with the following:

  Identify – Develop the organizational understanding to managecybersecurity risk to systems, assets, data, and capabilities.

  The activities in the Identify Function are foundational foreffective use of the Framework. Understanding the businesscontext, the resources that support critical functions, therelated cybersecurity risks, and ***the overall effectiveness***

ofcybersecurity activities that support the cybersecurity riskmanagement strategy enables an organization to focus andprioritize its efforts, consistent with its risk managementstrategy and business needs**.**

- Replace the existing paragraph describing Detect at lines 314 to316 with the following:

  Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. ***Similar to the Identify Function, the Detect Function requires a systemic approach to cybersecurity resource allocation. The Detect Function, being more complex than the Identify Function, requires cohesive and efficient coordination across multiple Framework categories and subcategories. This systemic approach enables optimization of each Detect Function cybersecurity activity, maximizing the overall effectiveness the Detect Function, and enabling implementation of the Detect Function within organizational budgets.***

2.2 Framework Implementation Tiers

- Add the following sentence to the Adaptive tier at line 424:

  A systemic approach to cybersecurity implementation will optimize the continuous improvement process by enabling timely, cost-effective, and accelerated insertion of advanced cybersecurity technologies into the organization.

4.0 Measuring and Demonstrating Cybersecurity

- Add the following paragraphs to the measurement anddemonstrating cybersecurity introduction at line 768:

  When aligning the measurement system with business requirements, costs must be contained despite the complicated nature of modern IT systems, and the interconnectivity between the IT system and external systems. In some cases, there will be a well-defined network edge. In others, interconnected systems will share access to sensitive resources. As the number of devices, data throughput and data diversity continues to grow, measurement costs can only be contained when an organization employs a cohesive and optimized measurement system to support determination of cause-and-effect.

  To implement a cost-effective and repeatable process for determination of cause-and-effect relationships, use of an abstraction layer that separates a dedicated measurement function from the analysis function will reduce cost while increasing measurement accuracy, and will contain the cost of the measurement function as

the need for additional analysis grows with the number of devices and the volume and diversity of traffic.