Cyber RiskScope®

www.CyberRiskScope.com

February 23, 2016

From: Robert Dowling, Product Manager, Cyber Risk Management Solutions, Dynetics, Inc.

Subject: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dynetics is an engineering solutions provider with over 40 years' experience supporting defense, intelligence and aerospace missions and over 16 years' experience providing information security solutions to government and private industry customers. Today, Dynetics offers Cyber RiskScope® as a portfolio of cyber risk-management solutions. The Cyber RiskScope methodology maps identified cyber risks to the NIST Framework for Improving Critical Infrastructure Cybersecurity (Framework) as an effective means of communicating cyber risk to clients.

As the Framework emerged, Dynetics recognized its value in creating a common lexicon by which organizations could consider desired cyber risk-management outcomes without requiring compliance to a particular standard or affecting adherence to an existing standard. This flexibility enables cyber risk-management companies like Dynetics to create common approaches for assessing cyber risk that can be applied across industry verticals without affecting their existing governance programs. For organizations with no regulatory requirements, the Framework provides an efficient means to assess their current and desired cyber risk postures. We have heard from numerous organizations without a cybersecurity governance requirement that, based on the maturity and size of their cyber risk organizations, traditional standards such as NIST 800-53 or ISO-27000 are overwhelming. Whereas the Framework is flexible, adaptable and therefore manageable. This fact alone likely means more organization are assessing their cyber risks than before the Framework existed.

Dynetics views this flexibility as an essential element to encouraging more organization to assess their cyber risk using a systematic approach. While the initial assessment may not be as thorough as would have been required by a compliance standard, organizations can at least establish a baseline from which to make improvements.

In addition, Dynetics believes that voluntary adoption of the Framework is essential to its effectiveness in fostering effective security. As soon as a requirement is defined, organizations begin focusing on the minimum required to comply rather than the means to achieve effective cybersecurity. Dynetics uses the voluntary nature of the Framework to promote to organizations that they achieve "enough" cybersecurity to mitigate anticipated threats. This natural extension of the Framework keeps clients focused on effective cybersecurity rather than compliance.

Dynetics

Dynetics has also leveraged the Framework to develop an affordable, online cyber risk assessment. Users are led through a series of multiple-choice questions that are organized around the five Framework Functions. Upon completing the online survey, users are provided with feedback on the effectiveness of the cyber risk-management program; and the feedback is mapped to the Framework Functions, Categories and Subcategories so that user can see how well they are achieving the outcomes defined by the Framework. Automated, low-cost assessments can help promote broader and quicker adoption of the Framework as even users with limited exposure to cyber risk frameworks can quickly visualize their cyber risk in the terms defined by the Framework.

In summary, Dynetics uses the NIST Framework for Improving Critical Infrastructure Cybersecurity to help clients manage their cyber risk. For the Framework to continue to be effective, it must

1. remain flexible to allow broad adoption,
2. remain voluntary to keep organizations focused on effective cybersecurity rather than compliance, and
3. remain extendable to motivate private industry to create solutions that promote continued focus and improvement in cyber risk-management.