From: Phil Wilson
Sent: Friday, December 29, 2017 7:49 PM
To: cyberframework <cyberframework@nist.gov>
Cc: Phil Wilson <phil@GRCsphere.org>
Subject: Our Comments and Suggestions RE: NIST CSF Framework and Roadmap Version 1.1

Hello NIST CSF Team,
We would like to suggest the following amendments and additions to the Cybersecurity Framework (CSF) and Roadmap Version 1.1:

1. **Process Stubs** – The CSF, itself, provides us with a solid IDEF0 function model structure and decomposition based on FIPS 183.*

   The addition of "process stubs" (i.e. generally accepted process models that can be tailored by an organization) would be especially helpful. The proposed process stubs would extend the CSF to address the next level of need for more detailed process models. We can't seem to find these and our members need help with this.

   We suggest that "role-based process flow models" be added using the well accepted ***Rummler Brache modeling methodology notation*** be used (also known as swimmer lane process models) or the ***IDEF3 modeling methodology notation***.

   *In Dec 1993 the National Institute of Standards and Technology announcing the standard for **Integration Definition for Function Modeling** (**IDEF0**) in the category Software Standard, Modeling Techniques. This publication announces the adoption of the IDEF0 as a Federal Information Processing Standard (FIPS) 183 as found here: http://www.idef.com/wp-content/uploads/2016/02/idef0.pdf.

2. **Cybersecurity Capabilities Measurement using Regression Modeling** – Currently, NIST provides a regression modeling capability for assessing probability of a risk event.

   https://www.nist.gov/services-resources/software/recipe

   Our organization would like to provide NIST with validated regression models under the Federal Reserve's SR-11 Model Risk Management standard which would be of significant help to industry. These models can be used to educate Board of Directors and C-level executives in a way that is not taking place today on a widespread basis, and should be based on the work by insurers in other measurement areas of substantial risk.

3. **Cybersecurity Capabilities Measurement using Industry Benchmarking and Indexing** – In addition to the use of regression models to help companies, we can further the benefit of cybersecurity breach analytics by adding industry benchmarking to provide companies with "peer average" and "best-in-class"

performance measurement along with public company indexing using our CyberRanking measurement of "**Cybersecurity Convergence™**" ; our term for the shift that a company consciously makes by taking cyber-related practices which have been classically used a defense mechanism and positioning them as a sustainable competitive advantage for the core business. Our measurement background uniquely qualifies us to measure Cybersecurity Convergence from a Strategic Shareholder Value perspective in a way that is both mathematically valid and has major ramification for insurance underwriters. We'd like to team with NIST on the use of our **CyberRanking™** and **Cognitive Benchmarking™** intellectual property measurements which use 5 year rolling averages for publicly-traded companies listed on US exchanges.

Thank you, in advance, for your consideration of these suggestions.

Thanks and Best Regards,

Phil

Phil Wilson
Executive Director
The GRC Sphere