Summary of Workshop and Next Steps

October 30th, 2014

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Thank You

- Florida Center for Cybersecurity
- University of South Florida
- Participants (in-person and webcast)

Workshop Objectives

- Understand stakeholder awareness of the Framework.
- Discuss initial experiences with the Framework.
- Identify tools, resources, and related activities to support more effective use of the Framework in order to help organizations manage risk.

What We Heard – Awareness of the Framework

- Strong awareness... but more is needed
- Shared responsibility for increasing awareness
- The Framework has promoted communication within organizations and across sectors
- Agreement on terminology remains an issue
- Too early for version 2.0

What We Heard – Experiences with the Framework

- Helpful in raising awareness and increasing/improving dialog with executive leadership
- Helpful in pulling people together across the enterprise
- Framework is being used in a variety of different ways
- Framework Core is where most organizations are focusing
- Framework Implementation Tiers are not well understood
- Mappings are being widely used to demonstrate alignment

What We Heard – Supporting Tools and Resources

- Desire for more illustrative “applications” of the Framework
- “Getting started” guides could be helpful
- Value of reference tools to express the Framework in multiple ways, understand the informative references, and aid in developing profiles
- Interest in a repository for hosting guides, sample templates, and other resources
- Additional work through the Commerce’s Internet Policy Task Force

What We Heard – Topic Working Sessions

- Authentication
  - Identity Management and Authentication are important to meeting cybersecurity goals
  - How to get there needs to be tailored to the priorities of the organization

- Privacy Methodology
  - Privacy still viewed as a bolt-on and the distinction between a privacy risk and a security risk is unclear
  - Expand participants to include privacy folks (“bring your privacy buddy”)
  - Broaden focus to managing privacy risk arising out of cybersecurity measures being conducted

- Cybersecurity Workforce
  - Critical to connect educators to industry (the classroom to the job)
  - Attracting and retaining a multidisciplinary cybersecurity workforce is critical

What We Heard – Topic Working Sessions

- Standards Supporting the Framework
  - Current approach allows for alignment
  - Balance reducing complexity while providing guidance

- Supply Chain and Conformity Assessment
  - Further clarity around terminology and concepts with respect to compliance, conformance, and confidence is needed
  - SCRM is broad and complex, and further research could benefit the broader community as well as specific sectors

- Automated Indicator Sharing
  - Threat intelligence requires context to be actionable, integrated into an organization’s workflow and risk management practices
  - The size and sophistication of an organization determines, to a large extent, the threat information it can use.

What’s Next…

- Analyze feedback and input received through the RFI and the Workshop
- Publish a post-workshop status update
- Continue focus on awareness across sectors and internationally
- Continue work on roadmap items
- Continue to explore options for future governance of the Framework

Stay Engaged

- *Framework for Improving Critical Infrastructure Cybersecurity*, available at www.nist.gov/cyberframework
    - Please send us your notes, continued observations, further suggestions, and share your Framework experiences at cyberframework@nist.gov

- Participate in our cybersecurity workshops and comment on our standards and guidelines

- Follow our cybersecurity activities at http://csrc.nist.gov

- Participate in the DHS C3 Voluntary Program events and webinars
    - https://www.us-cert.gov/ccubedvp