April 7, 2013

Author:
Russell Cameron Thomas
PhD Candidate
Department of Computational Social Science
George Mason University
Fairfax, VA
Email: russell.thomas@meritology.com
Bio: http://www.css.gmu.edu/?q=node/104
Twitter: @MrMeritology
Blog: http://newschoolsecurity.com/author/russell/

Submission to NIST RFI for Critical Infrastructure Cyber Security Framework (CSF)

The aim of this submission is to challenge some of the fundamental assumptions and approaches of the CSF and to suggest alternatives that will better fulfill the objectives of the Executive Order[1] (EO) and the US National Strategy for Cyber Security[2].

Main Message

The US CSF should focus on evidence-based evaluation to accelerate continuous learning and innovation. The UK government is following this approach right now[3].

Recommendations

- From the perspective of organizational and institutional change to improve cyber security in critical infrastructure industries (CII), there are three core challenges:

    1. Complex interdependencies and emergent risks, including the possibility of cascading catastrophes
    2. The need for agility and rapid innovation, even in the face of severe uncertainties

[1] "Executive Order -- Improving Critical Infrastructure Cybersecurity", Feb. 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] The US National Strategy is summarized by documents on this web page: http://www.whitehouse.gov/cybersecurity.

[3] Cyber Security Organisational Standards—A call for views and evidence, March 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf

3. The forces that govern cyber security implementation, innovation and transformation are diffuse and widely distributed. They primarily involve incentives, mental models, organization routines, and cultural norms that resist top-down mandates.

- The idea that the CSF needs to be a compendium of prescriptive "cybersecurity standards, guidelines, frameworks, and best practices"[4] and that it should include "conformity assessment programs" is *fundamentally flawed and should be abandoned* because it won't address these core challenges. In fact, it might become an additional source of drag on change and innovation. Even if the outcome is mildly beneficial, this is not the highest and best use of government and private sector resources.

- There is no lack of standards or lists of "best" practices. Instead, the *biggest gap is the lack systematic evaluation of what "good" or "best" means* given information about the latest conditions and emerging trends. Today, most of what is called "good practice" or "best practice" today is nothing more than opinion that is repeated often enough by "thought leaders" that it becomes culturally accepted. There is almost no evidence or objective evaluation standing behind it. In terms of collective intelligence, this lack of evidence and objective evaluation means we don't learn fast enough or well enough. Worse yet, this gap perpetuates bad practices, mismanagement, blame shifting, excuses, and poor outcomes.

- Therefore, the CSF should instead focus on *institutional innovation* to support *evidence-based evaluation* of any and all standards, guidelines, technologies, and practices that are proposed by any sector – private industry, trade organizations, NGOs, international standards organizations, academics, or professional communities of practice. "Let a thousand practices bloom!"[5] Every organization or person who promotes a practice as "good" or "best" should have the burden of proof and should provide supporting evidence or objective evaluation. The best contribution of the CSF will be as the outside *learning loop* to ensure that practices are continually evaluated, improved, and then eventually discarded when they are no longer appropriate.

- The CSF should serve as a *nexus of experiments, pilots, test beds, data, evaluation resources, and open innovation communities* to support innovation in cyber security practices, especially through cross-sector and/or agile teams. The term "nexus" refers to activities such as funding, hosting, orchestrating, sponsoring, vetting, evaluating, and promoting. It also means tolerance for failure

[4] NIST Cyber Security Framework RFI, p 1.
[5] http://en.wiktionary.org/wiki/let_a_thousand_flowers_bloom

rates to support discovery of "out of the box" solutions. This CSF role would be in line with the US Cyber Security R&D Strategy[6], which includes "Incentives and Economics" as one of the four priority areas for "game-changing innovation".

- Rather than promoting "conformity" to consensus standards, the CSF should be promoting *responsibility* and *accountability*. For example, every organization in CII, including firms in their supply chain and service chain, should be held accountable for making on-going investments in evidence-based evaluation, including experiments, pilots, and simulations. The results should be publicly disclosed through the institutions provided by the CSF. Another example: every CII organization should bear financial responsibility for cyber risk using regimes similar to Operational Risk management in the financial sector (e.g. Basel III and Solvency II[7]). Ideally, the "cost of risk"[8] should be managed at a Board level, publicly disclosed, reflected in critical supplier and partner contracts, and tied to executive compensation. Of course, per the bullet points above, these need much more research and evaluation before they will be widely adopted, but they exemplify the sort of future state that will fulfill the EO and US National Strategy in a way that can "address [the] *constantly evolving* risks to critical infrastructure cybersecurity"[9].

- To support these goals, there are a small number of standards and compliance regimes that don't yet exist or need to be expanded. The CSF could make a significant contribution by defining a small number of standards for *information sharing*, *public disclosure*, and *organization/executive accountability*. These, in turn, would support legal and regulatory regimes involving the SEC, FTC, DOJ (anti-trust), OCC, DOE (NERC/FERC), as well as national and state legislation regarding mandated disclosure, privacy, civil liability, etc.

- Finally, given the CSF goals defined above, there is no benefit in the US acting alone or in isolation. Instead, the US CSF initiative should immediately *collaborate and/or integrate with similar initiatives in other countries* –UK[10], Europe, Canada, Finland, and Estonia, to name just a few. The primary benefit of collaboration and integration is pooling of resources (money, time, facilities) and pooling of expertise, which could lead to better results for everyone, and faster.

---

[6] http://www.nitrd.gov/fileupload/files/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf
[7] http://en.wikipedia.org/wiki/Basel_III, http://en.wikipedia.org/wiki/Solvency_II_Directive, http://www.johnthirlwell.co.uk/operational_risk_141010.pdf
[8] Society of Actuaries, 2010. A New Approach for Managing Operational Risk, Society of Actuaries. Available at: http://www.soa.org/files/research/projects/research-new-approach.pdf [Accessed January 29, 2013].
[9] NIST Cyber Security Framework, p 3, emphasis added.
[10] Cyber Security Organisational Standards—A call for views and evidence, March 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf