Developing a Framework to Improve Critical Infrastructure Cybersecurity

TOPIC: The Critical Security Controls and the Executive Order

RECOMMENDATION: The Critical Security Controls (CSCs), found at http://www.cyberaction.org , can and should play a significant role in the Framework to Improve Critical Infrastructure Cybersecurity. Here are some of the attributes of the CSCs that meet the intent of the Framework:

- they are developed and maintained by a large volunteer, consensus community
    - including government Agencies and the private sector, and cutting across many sectors of the economy
    - contributors span across technology, threat, vulnerability, offense, and defense
- they have broad, positive community acceptance by enterprises, vendors, consultants
    - voluntarily adopted by many enterprises in many sectors (e.g., multiple levels of government, finance, telecomm, power, transportation), and in many nations;
    - supported by numerous vendor with tools, white papers available (e.g., http://www.sans.org/critical-security-controls/vendor-solutions/)
- the CSCs were chosen based on their high value in stopping attacks - the primary goal is to bring priority and focus to countermeasures

- the CSCs enumerate specific actions, with a vendor-neutral approach
- they are demonstrably consistent with, and easily mappable to a subset of existing formal Risk Management Frameworks (e.g., FISMA, ISO27002), and to similar projects like the Australian DSD 35 (and their Top 4), and from the NSA
- studies in a variety of sectors (e.g., telecomm, power generation) have shown that the CSCs map naturally into a subset of existing security regulatory requirements
- they are demonstrably mappable as a solution set to specific threat information (e.g., The 2013 Verizon Data Breach Investigations Report will include a mapping from the problems highlighted in their Report into the solutions found in the Critical Security Controls)
- they are naturally supported with standards-based automation
- they easily align with "continuous monitoring" programs by identifying the highest priority defensive actions and the most important measures to be collected
    - DHS is using this approach to acquire government-wide technology for the "Top 4" Controls

In the attached paper, “The Critical Security Controls: The Foundation For An Enterprise Risk Management Framework”, I describe how the CSCs and their development are consistent with the formal Risk Management Framework of FISMA, and propose that the CSCs represent the outcome of a “foundational risk assessment” developed by a knowledgeable community instead of by an individual enterprise. Of course, the Critical Security Controls (or any set of Controls) do not constitute an entire framework as called for in the Executive Order. However, they do

offer a well-supported, baseline of specific high-value actions, supported by a broad community, and consistent with formal risk management frameworks.

thank you

Tony Sager
Director, The SANS Institute
Director, The Consortium for Cybersecurity Action