From: Michael Rich
Sent: Tuesday, March 1, 2022 4:19 PM
To: CSF-SCRM-RFI <CSF-SCRM-RFI@nist.gov>
Subject: RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Hi,

I'm very happy you are starting the updating process for CSF. I was wondering if I would need to move to a new framework. I have been using and assessing against the CSF framework for the past 4 years.

I recommend the following controls be eliminated or modified because I do not feel the measurably reduce risk. When I state "measurably reduce risk" I am referring to a quantifiable reduction in either probability of loss event or the magnitude of the loss. I have fully implemented quantitative risk methods (in the manner of FAIR or Hubbard's "How to Measure Anything in Cybersecurity Risk"). The controls listed below have no impact on my risk measurements.

They may be "nice to have" but they are distractions from controls with real impact on risk

- ID.BE-1: The organization's role in the supply chain is identified and communicated
    - Perhaps its just the "communicated" portion of this. I just don't see how the staff knowing where they are in the supply chain reduces risk
- ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
    - This is a managerial control for "team spirit" and has no impact on risk
- RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
    - In a sense I suppose this is an attempt to reduce risk to the entire industry, but it doesn't actually do that.
    - Many (most) companies do not allow openly sharing this info as a matter of liability control

My final comment is to not fall for the hype and do not include a "Zero Trust" control in the next iteration. This is a buzzword term with little consensus on meaning and no identifiable framework. If you must include concepts that come from discussions of "Zero Trust" please list the technical control specifically and do not just put: "Implement Zero Trust". Try something like: "All applications must positively assert authentication"

Thank you for your time