Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Paul Wertz and Lan Jenson

NIST GCTC-Smart Secure Cities and Communities Challenge: Smart Security and Privacy (SSP)

April 25, 2022

Comments:

1. Discussion on Gaps that in supply chain since the 2018 document:
   - Oftentimes a stark lack of understanding of requirements as described and focusing on high level security control and not overall objectives or goals that may give a false level of security.
   - How nascent cyber liability transfer is between two companies that work together (this may include the U.S. Government) for a similar objective. This can often include infrastructures up to and including city infrastructure.
   - What level of adoption of the GCTC documents have been codified into solicitations over the past two years and the resulting assessments – have issues been addressed either by the implementing authorities, or the bidding vendors that may win.
   - Who is responsible to verify that issues have been addressed appropriately?
2. What blind spots does the CSF have and what mechanism is in place to validate vendors' self-attestation. Since the supplier performance risk system doesn't have a central repository for Smart Cities executives to reference, problems can be easily overlooked. This can lead to purposeful or negligent assessments and the resulting implementation.
3. Adoption of the NIST methodology can oftentimes lead to architecture that isn't necessary current and how is it to be looked at with fresh eyes to attend to updates over the past several years (can you see certain things, can you accomplish things, etc.). Especially when using document to create a 'how to' program in today's environment.
4. How are the various other reference documents (800-171, 800-160) to be incorporated or operationalized?
   - How do you prioritize the different objectives?
   - Are there criticality components that might impact the way a solution may be implemented.
   - Different assets have multiple hops and connections and how are recommendations developed under the framework.
5. Is the going to be a push for CISO inclusion or security aspects to be represented to the C-Suite (as recently suggested the SEC) – does the CBS score have to be implemented or prioritized the same across the network. Can the risk value be quantified in a consistent business manner?
6. In patching the devices how do you prevent creating an administrative nightmare across various groups in various environments.
   - In this situation, how do you really define current?

    - There was also some discussion as to whether this is meant to be a living document or a static document?
    - Do you only need to be worried about security relevant patches?
    - There seems to be an assumption that there is a sandbox and not a live environment. There needs to be other ways to possibly address.
    - Can a virtual desktop environment be used to control the deployed resources?
    - There is a perceived gap between the framework and when individuals go to implement in an operational environment.

7. If NIST says the framework is the only guide, can we have a more active relationship to address scalable efforts to assist local governments with a sort of template that give a much better starting point.
    - What kind of controls are there for addressing sitting endpoints over time and getting the patches out versus just pushing out a new image?
    - Who will ultimately be held accountable?
    - Might there develop levels of certification, maybe a gold, silver or bronze that companies may pay for?
    - Would Blockchain possibly be able to provide a controlled environment to verify software components?
    - As the IT/OT world converges, this level of security will become more critical.
8. What issues has remote work due to COVID-19 exacerbated?
    - Have company's deployment practices created new problems, and how is this impacting the cost of doing business.
    - What is the Board of Directors involvement, and what should it really be?
    - Are new groups of remote workers bringing to light different areas of concern?
    - Documentation and evolution of best practices for day-to-day use, boardroom involvement and legal defense.

In summary, the feeling was that this space is a rapidly evolving space that needs to address a wide spectrum of concerns and prevent stove piping of data. This necessarily begins with internal assessment moving out to the network edges and ultimately including all components, software, solution providers and users. This initiative needs to be better communicated to businesses for implementation. Massive adoption through collaboration across federal agencies needs to become a priority.

Websites mentioned in the discussion:

https://en.wikipedia.org/wiki/SUBSAFE

https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-manufacturers

Background

The Smart Security & Privacy supercluster (SSP) is a public private partnership that supports NIST GCTC Smart Secure Cities and Communities Challenge https://pages.nist.gov/GCTC/. SSP held a virtual meeting attended by 20 participants to discuss public input on Consumer Cybersecurity Labeling for IoT products on December 14th,2021, The participants represented a wide variety of interests including individuals with experience in business development, software development, network management, software deployment, and consumer engagement. We had private, government and non-profit points of view represented.

https://smartsecurityprivacy.org/

https://www.linkedin.com/company/nistgctcsmartsecurityprivacy/