Strengthening Resilience: Incorporating Cyber Continuity Into NIST's Cybersecurity Framework 2.0

In response to the National Institute of Standards and Technology's ("NIST") Public Draft of its Cybersecurity Framework 2.0's ("CSF 2.0"), I recommend the National Institute of Standards and Technology (NIST) integrate comprehensive continuity elements and guidance into the final release of its Cybersecurity Framework 2.0 (CSF 2.0).

What is Cyber Continuity?
Loosely defined, cyber continuity entails developing plans, processes, and procedures that ensure the continuation of critical service delivery during a cyber incident affecting IT/OT systems. It requires considering both technical and non-technical alternatives to maintain essential operations when standard systems fail.

Why Should NIST Include Cyber Continuity in the CSF 2.0?
The escalating reliance on technology, particularly sophisticated systems like Artificial Intelligence, necessitates cyber continuity measures. As technology increasingly underpins our operations, maintaining business or mission functions during cyber attacks becomes imperative. Entities such as schools, hospitals, and the electric grid must prioritize their mission-critical and business-critical functions, as cyber incidents have or could lead to significant disruptions in essential services.

The importance of cyber continuity cannot be overstated. As CISA Director Easterly recently emphasized in a recent blog post, resilience is about proactive preparation for disruption, with a deliberate focus on continuity and recovery. This approach not only prepares organizations for the inevitability of cyber incidents but also enhances their ability to operate in a degraded state and significantly reduces downtime when incidents occur.

Cyber continuity also follows the same logic as zero trust, which acknowledges the inevitability of attacks and incidents. Organizations must prepare for the worst-case scenarios and ensure the continuity of core functions.

How Should NIST Incorporate Cyber Continuity into the CSF 2.0?
NIST could establish cyber continuity as an independent function or weave it into the response function—or even throughout multiple functions of the framework. However it's done, It is vital to provide more continuity consideration and guidance. Here are a few key recommended principles or actions:

- **Maintain Critical Services/Functions**: Formulate contingency plans to uphold critical services during a cyber incident. Organizations should prioritize continuity planning and capabilities for the most critical systems and services. These plans must address scenarios involving partial or complete loss of IT/OT systems and should include non-technical alternatives. Prioritization should go to services crucial for public safety, health, and economic stability.

- **Communicate Service Impacts**: Implement systems to alert the public and stakeholders about service disruptions, offer updates, and outline alternative services, particularly when a cyber incident disrupts communication channels.

- **Build Redundant Systems**: Create redundancy in IT/OT systems supporting critical services to ensure backup systems and data can seamlessly activate if primary systems are compromised. Achieve redundancy through cloud computing, non-technical policies, and other means.

- **Exercise and Evaluate Contingency Plans**: Conduct regular tests of contingency plans to ensure all participants understand their roles and can carry out alternative processes. These drills are essential for spotting planning deficiencies and are a fundamental part of the "test, analyze, and learn" strategy from the response phase.

Further actions to strengthen cyber continuity include:

- Developing Continuity of Operations Plans (COOP)
- Crafting contingency plans for various scenarios
- Forming mutual aid agreements for resource sharing in crises
- Securing emergency/backup contracts for swift resource acquisition
- Establishing data backup plans and policies to maintain data integrity and availability

I also suggest that NIST review the G20 Smart Cities Alliance's Cyber Resilience Model Policy, which has modified the NIST CSF to include a Sustain Function for continuity. You can find more information on this policy here: G20 Smart Cities Alliance Cyber Resilience Model Policy.

Thanks,
Christopher Covino