October 10, 2014

Diane Honeycutt
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Stop 8930
Gaithersburg
MD 20899

RE: Experiences with the Framework for Improving Critical Infrastructure
Cybersecurity

Dear Ms. Honeycutt,

I am writing in response to the request for information regarding the level of awareness in critical infrastructure organizations of the Framework for Improving Critical Infrastructure Cybersecurity (the Framework).

Represented in this RFI response is the perspective of professionals skilled in **Business Continuity (BC) , Disaster Recovery (DR) and Crisis Communication.** These professionals are responsible for coordinating business response to major physical and technology disruption events. These professionals work with critical business, technology teams and third party vendors to prepare for significant threats and develop contingency plans to reduce the impact of threats on their businesses and customers. The Framework roadmap may want to consider Business Continuity practices to expedite cyber event response planning and support a company's implementation of the Framework controls.

Information used as the basis for these findings has been gathered from multiple educational workshops, conference presentations, industry polling and a pilot program, which applied the Framework to a small financial services entity.

Since the inception of the Framework, I have worked with colleagues to align the Framework with an operation's business-as-usual and business continuity routines. Although the Framework is voluntary, observations presented in this document reflect the experiences of some individuals working for regulated organizations. In their work roles, they have been preparing for, or have been participating in, the regulatory examinations of their organization's third party practices and cybersecurity readiness.

AWARENESS OF THE FRAMEWORK

Boards of Directors have been made aware of their oversight responsibilities for cybersecurity through various sources. This awareness has driven change in many organizations. Change includes organizational realignment to increase business responsibility for cybersecurity risk. Governance of cybersecurity risk is being expanded. Many business continuity professionals have reported that they are not included in Framework discussions, within their organizations, however, they anticipate this to change. Consistent feedback was received that there is a prevailing viewpoint voiced that Information Security (Info Sec) personnel and the Chief Information Security Officer (CISO) within their companies are "taking care of this". In some cases, professionals are aware of their risk management organizations increasing cybersecurity risk assessment and activity mitigation.

Analysis of Framework adoption and current awareness may benefit by observing an individual's emotional reaction to the subject. When first shown the sub-categories and controls of the Framework, people outside of the Information Security field hesitate, perhaps, from a perception of complex technical and unknown skills. This attitude can change when business leaders are provided logical examples for Framework controls, or shown how controls work together, by using the example of a kill chain analysis report. Leaders become engaged and debate activities for contingency planning and smarter business practices. Comments from the BC community called for more awareness of security practices to guide the development of cyber threat contingency plans.

INITIAL EXPERIENCES

I. Change Instigated by the Framework:

1. There are significant increases of internal security risk assessments.

2. Deeper dives into evidence testing on third party vendors are taking place.

3. Organizations are analyzing the impact of cybersecurity risk to other areas of corporate risk: market risk, credit risk, supply chain risk, legal risk, operational risk, systemic risk, etc.

4. Organizations are debating how structural alignment will create effective cybersecurity oversight and improve collaboration between departments that contribute to risk mitigation and control quality.

5. There is increased staff & contractor hiring taking place to support cybersecurity risk activities.

II. Industry implementation challenges:

1. Small businesses competitiveness depends on the usage of third party partners. It will be challenging to incorporate the Framework risk management practices into existing partnerships, contracts and service level performance measurements.

2. Small businesses hire independent and small business contractors that are not consistently being trained in the Framework controls. There is a knowledge gap.

3. The Framework and Info Security have not consistently engaged business response activities into cybersecurity incident command. They can, but have not consistently integrated BC crisis communication practices that contain business monitoring, trigger events and escalation activities.

4. Reducing third-party and supplier cybersecurity risk presents the potential to reverse important cost efficient operational practices and competitive strategies. This will be a critical area of discussion as leaders seek to apply the Framework and define their third-party cybersecurity risk appetite.

III. <u>General Comments on Cybersecurity Risk Strengthening:</u>

1. Everyone needs to own cybersecurity risk and not just differ ownership to Info Security or Technology. There is a need to increase the engagement of business leaders in the development of cyber crisis response plans.

2. There is no clear direction being communicated on how to apply the Framework. This is not stopping some organizations from mapping Framework risk activities to their existing operational procedures.

3. People don't want to hear about "maturity model" for multiple reasons. The term is perceived as prescriptive, expensive and will create a barrier to Framework usage.

4. There is a critical need to engage business leadership and realistically address the attitude that security is "someone else's job".

5. Each company should create an enterprise wide cyber event response plan as soon as possible. This process can be facilitated through the company's Business Continuity program.

6. Many Framework activities and controls require multi-department collaboration to implement and sustain the effectiveness of the security activities. Territorial battles are reported as barriers to this collaboration. Some companies point to recent organizational realignment to address these barriers.

7. Business Continuity exercises need to be scaled up to illustrate the effects of a cybersecurity physical attack. Characteristics of the exercise should include realistic detail to encourage participation of critical employees During cyber exercise workshops, participants suggested the following ideas:

    a. Create a complex and multi-regional cyber event scenario that combines the physical damages and interdependent failure scenarios of a hurricane, like Super-storm Sandy, with critical infrastructure disruptions.

    b. Exercise objectives should include the development of threshold monitoring that can be used by Information Security to trigger increased communication to critical business teams during a cyber event and facilitate business contingency plan activation.

    c. Include in the test scenario, challenges in vendor communication and critical 3rd party system failures.

    d. Require critical staff physically move to their alternative work locations during the exercise in order to increase their recognition of the seriousness of planning. During the exercise, discuss different cyber attack impacts that may disrupt their current contingency plans, including, access to their alternative work locations.

    e. Transfer critical systems to the alternative work site and have staff process transactions. Discuss how Internet disruption during a cyber attack would impact critical systems.

    f. Include intermittent telecom and power disruption along with physical event disruption.

In closing, the purpose of this communication is to share opinions of the NIST Cybersecurity Risk Framework, version 1.0, gathered from the community of Business Continuity professionals. These individuals work within their businesses to implement resilient systems and business disruption event contingency planning.

Thank you for this opportunity.

Susan Rogers, MBCP, MBCI
CEO
Cyberwise CP