NIST CSF 2.0 Concept Paper request for feedback – due 3/3/2022

Cowbell applauds the body of work already done around version 2.0 of the NIST CSF and would like to provide high-level inputs as listed below.

As a provider of cyber insurance to small and mid-size enterprises (SMEs) with revenue under $1 Billion, we rely on existing cybersecurity assessment methodologies to understand and price cyber risk for the businesses ("the insureds") that transfer risk to Cowbell. Our risk modeling approach has been specifically designed for insurance purposes and relies on the current NIST CSF framework.

- **1.2 Scope of the CSF to ensure it benefits organizations regardless of sector, type, or size**
  SMEs are the least equipped to deal with cybersecurity challenges. They have to focus on their core business and lack the resources (budget and people) to proactively address cyber threats let alone respond to a cyber incident. Education and preparedness in the SME market is paramount and can be the difference between an insignificant or devastating cyber incident. There are more than 30 million SMEs in the U.S. and these companies often make the backbone of the supply chain of larger companies that might be critical infrastructure.
  We welcome any revision of the framework that makes it easily adaptable by SMEs, through either simplification, the availability of templates, or even the sharing of examples of how SMEs can successfully adapt the framework.
  (Paragraphs related to the above: 3.1 – Add implementation examples of CSF subcategories; 3.2 – Develop a CSF Profile Template

- **2.6 Remain technology and vendor-neutral, but reflect changes in cybersecurity practices**
  Not all technology solutions are created equal and for some of the most widely used infrastructure technologies, we see an opportunity to leverage some of the work already pursued by various entities. For example, the CIS (Center for Internet Security) benchmark for Microsoft, AWS, and other technology solutions provides a great starting point for SMEs to apply security best practices more systematically.

- **4.2 Improve discussion of the relationship with risk management**
  Assessing risk is at the core of insurance. In the case of cyber risk, the insurance industry as a whole and Cowbell, in particular, are pursuing means to evolve static (most often meaning yearly) approaches to risk assessment to models that are a lot more dynamic (even continuous in the case of Cowbell) so that risk transfer mechanisms through insurance remain closely aligned with the actual risk faced by insureds and covered.

- **5.1 Expand risk to cover the supply chain**
  Cowbell absolutely welcomes the focus on the supply chain. There is a potential need to differentiate between

(1) **The software supply chain,** the dependency from many businesses on a variety of software technologies which themselves might carry a broad range of vulnerabilities.
(2) **Third-party vendors that are not software or technology providers.** The security practices of third-party (and even fourth-party) vendors inherently contribute to the cybersecurity and cyber risk posture of many organizations.

At Cowbell, we have introduced models to evaluate the exposure of our policyholders to software supply chain risks but welcome the development of a robust, all-encompassing model for such risk.

- Other:
  (1) **MSP/MSSPs:** we would also welcome the inclusion of MSPs (Managed Service Providers) and MSSPs (Managed Security Service Providers) in the revision work conducted for the 2.0 version of the CSF.

  The team at Cowbell welcomes the opportunity to discuss any of the above comments if needed.

  The Cowbell Team.