RSA Conference 2018

NOW MATTERS

Peer2Peer

Cybersecurity Framework 1.1 Adoption Experiences and Opportunities

P2P3-T10: Cybersecurity Framework 1.1 Adoption Experiences and Opportunities

Timothy Shea Global Public Sector, RSA

The NIST Cybersecurity Framework https://www.nist.gov/cyberframework was released in February 2014. At the 2015 RSA Conference I hosted a peer-to-peer (P2P) session on the framework: Cybersecurity Framework - Adoption Experiences and Opportunities. While the room was full, including participation from NIST - conveyors of the Framework – there were very few people who had implemented the Framework, but many who planned to. Also in attendance were a number of consultants who were, undoubtedly, trying to understand how they could wrap their services around the Framework.

Fast forward to RSA Conference 2018 where I hosted two sessions on the Framework, both titled Cybersecurity Framework 1.1 Adoption Experiences and Opportunities. To be fair, version 1.1 of the Framework was released on Monday of Conference week so our 'experiences' conversation focused on the 1.0 release. The fact that we had two full sessions on the topic illustrates the increased level of adoption of the Framework.

The attendees fell into three buckets: organizations who had implemented the Framework; consultants; and those looking to learn. We had a large number of Framework adopters included one of the largest cities in the U.S., several major petroleum companies, an Agency of the U.S. Government, a large investment management organization, internationally-based organizations and a number of midsized companies.

The participating consultants had built practices around the Framework and were able to offer useful insight into a variety of implementations of the Framework.

Finally, there were those who came to learn. These folks appeared to be from mid-sized organizations. We also had the government of an Asian country who was comparing the NIST Framework to ISO standards with the intent of picking one for their national standard. Interestingly, although the Framework was developed for U.S. critical infrastructure, half of the attendees represented non-critical infrastructure or non-U.S. based organizations!

Comparing the 2018 sessions to my 2015 session the obvious differences were the level of adoption and the level of experience the attendees had with the Framework. The nature of the questions was different as well. Three years ago, folks wanted to discuss what the Framework was and how to implement it. Interestingly, this year we drilled down into the benefits, how to sell Framework implementation to management and what internal alliances/partners were needed to successfully deploy and leverage the Framework.

For those who implemented the Framework, well, they implemented the NIST Cybersecurity Framework as a framework! Every one of them modified the Framework to their specific business or mission requirements. Examples include:

- Modifying the number of tiers
- Providing a weighting mechanism to the Functions, Categories and Sub-Categories - the idea being that not all Functions, Categories and Sub-Categories are created equal. For example, a GAP of ‘X’ in the function of Identify may be more important to close than the same GAP of ‘X’ in the function Respond. Why? Because the ability to identify assets and threats is foundational to any cyber risk management program.
- Associating investment dollars to the GAP analysis
- Deploying lighter and heavier weight versions of the Framework across business units, depending on the unique requirements and cyber risk maturity of those business units. An example of lighter and heavier weight would be using just Function and Category (lighter) and Functions, Categories and Sub-Categories (heavier)
- Implementing additional informative references
- Several companies used the Framework on top of their existing cyber risk management tool(s) for the express purpose of translating “cyber speak” to “business speak”

The first question from the P2P group was “what is the value of another framework, why is this different”? As a team, we discussed the benefits of the Framework to include that this Framework provides metrics and a lexicon with which to describe a cyber risk management program and, more importantly, to describe cyber risk management in the language of the ‘C’ suite and board of directors. This dovetails nicely with the fact that the ‘C’ suite and board are realizing that cyber risk must be governed by the same processes as other significant business risks.

The question of how to sell the Framework to management and what internal partners are needed are intertwined. Why? Well, for cyber practitioners (those in the P2P session), alignment with internal business partners is key to articulating the value of a cyber risk management program to the organization’s leaders. As an example, a great business partner could be the head of a business unit, especially one who conducted customer facing E-commerce. The business unit head would generally also be aligned with the larger governance structure within an organization. Alignment with legal was top of mind. Legal cares about risk and has a seat at the table. This is also true with audit teams due to their ability to compel business units to comply with audit requests.

For me, it was wonderful to see members of the P2P groups connecting and sharing their experiences and their contact information with one another. I know that the value of the P2P session extends beyond the 45 minutes we spent together at RSA Conference 2018!