Current Awareness of the Cybersecurity Framework

Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness, NIST solicits information about awareness of the Framework and its intended uses among organizations.

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

   From our experience there definitely appears to be awareness of the Framework among multiple industries and areas. There is a lot of current analysis ongoing, but evidence of full implementation is unclear. Within Virginia we found the Framework easy to both analyze and adopt.

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

   In addition to the many news articles and outreach from NIST itself we've seen a lot of discussion in conferences and events.

3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

   Virginia has provided information a number of times to different audiences about how the state has implemented the Framework and some of the lessons learned from that implementation. Some critical infrastructure organizations were included part of those audiences.

4. Is there general awareness that the Framework:

   a. Is intended for voluntary use?

      The fact that it is for voluntary use has been mentioned within most of the literature and presentations that we've seen. The organizations that we've interfaced with while discussing the Framework also seem to understand that it is voluntary.

   b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

      Conversations have not clearly indicated one way or another that organizations understand how to integrate into their risk management program. Every discussion that we've had about the Framework has included information stating that it should be integrated into an organizations risk management framework.

   c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

From our discussions it isn’t currently clear to us how other organizations are going to implement the Framework. There has been a lot of effort put into analysis and understanding. We haven’t had a lot of people share their implementation story with us yet.

5. What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

   The greatest challenge will likely be on how to show the results/benefits of implementation. Conceptually it makes sense and there appears to be a lot of traction getting started, but over time there will probably be a request for proof of improvement. How to represent that improvement will be important since organizations will need to represent the results in a comparable fashion.

6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

   We haven’t spoken with international organizations regarding the Framework.

7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

   There is definitely awareness within the state, but we aren’t directly regulated excluding federal government requirements. The federal government is definitely aware.

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

   Yes, we have presented to many different public and private sector organizations as well as contributed to articles and press releases.

9. What more can and should be done to raise awareness?

   At some point showing the improvement/results of implementation will help raise awareness of the Framework benefits.

Experiences With the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

1. Has the Framework helped organizations understand the importance of managing cyber risk?

The Framework has definitely helped to raise awareness and bring focus to the fact that cyber security is part of managing risk. It helps with creating a common risk language between parties which also helps with understanding risk.

2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?

   Within the Commonwealth of Virginia we have already implemented the Framework. We've spoken to some partner critical infrastructure organizations who are considering adoption, but we haven't had anyone come out and commit to it.

3. What benefits have been realized by early experiences with the Framework?

   The largest benefit is the common language spoken between parties. Our organization is able to effectively communicate a summary picture regarding the status of information security programs.

4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

   One of the largest challenges we've run into is a suggested way to visually represent the data. Using that information would help for immediate understanding of the level of risk an organization carries and would hopefully allow for better risk decisions.

5. Do organizations in some sectors require some type of sector specific guidance prior to use?

   I don't know that we are able to make a determination one way or another regarding this question. It doesn't appear that there is need for much specific guidance considering the Framework is based on industry standard controls.

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

   That is how the Commonwealth of Virginia approached it and that is also how we have recommended implementing the Framework when discussing it with other organizations.

7. Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

   The largest struggle that we've experienced has been with the implementation tiers. While there is a description of each tier there is a lot of room for subjectivity and not an easy way to represent progress in a tier. The rest of the components worked out very well and were easy to integrate into our existing risk program.

8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.
   a. Of these recommended practices, how are organizations initially using the Framework?

We’ve followed some of the steps in the recommended practices since we already completed some of the steps. It would likely be helpful if there were more steps surrounding how to integrate into an existing risk management framework in addition to using it to start a brand new information security program.

b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

   Not that we’ve experienced.

c. Are organizations leveraging Section 3.5 of the Framework (“Methodology to Protect Privacy and Civil Liberties”) and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

   We aren’t in a good position to answer this question. We have some privacy rules in place that are legislatively designated and others that previously existed.

d. Are organizations changing their cybersecurity governance as a result of the Framework?

   We made some tweaks to our governance to accommodate the Framework, but due to the flexibility of the document we did not need to make many.

e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

   We included a first attempt at our results when putting together our annual security report. We used a graphical representation of the results to communicate to our stakeholders. We want to refine the process further before we integrate it into all of our communications but it has been used.

f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

   We have not used the Framework to do this yet, however we are interested in using it to understand the state of an organizations security posture. We have security standards that third parties typically have to follow.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

   Using the Framework as a common way to report the status of an organizations cyber program would be a great way to promote implementation.

10. Have organizations developed practices to assist in use of the Framework?

We utilized the information provided in the Framework. We have not been exposed to other practices that would assist in use.

Roadmap for the Future of the Cybersecurity Framework

NIST published a Roadmap [6] in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?

   The areas included in the roadmap are all significant factors within cybersecurity and need to be addressed.

2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?

   Focusing on a way for organizations to communicate with one another is one of the major benefits of the Framework. It would be great to make sure that is taken into account when continuing to develop the Framework.

3. Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?