threat SKETCH℠

January 19, 2018

Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 2000
Gaithersburg, MD 20899

Re: Comments on The Framework for Improving Critical Infrastructure Cybersecurity,
Version 1.1 Draft 2

Ms. Arbelaez,

First, let me first thank all of the contributors to the NIST Cybersecurity Framework (CSF) for a job well done. The framework continues to provide much needed cohesion among national and international stakeholders in every sector. I hope you find my comments, which are primarily about the roadmap, helpful.

**Risk Transfer and Risk Pooling**

Please consider adding risk transfer and risk pooling to the roadmap as a topics for study. Risk transfer implies that someone else accepts liability, which is driven through contractual, statutory, or regulatory means. Risk transfer is generally the domain of attorneys, who play an important role in cyber risk management in addition to traditional IT folks.

Risk pooling refers to a classic insurance function in which multiple potential victims come together to share a low probability, high impact risk. Everyone chips in to the “pool” and the one that gets attacked gets to withdraw funds to cover the loss. Pooling through cyber Insurance, etc. plays an important role in managing certain types of cyber risk.

**Opportunities Within Cyber Risk Management**

Another topic to consider adding to the roadmap for further research is finding opportunities within the risk landscape. Managing risk is not just about mitigating downside, there is also an upside component. As a bonus, identifying opportunities requires engaging a more diverse organizational team. Having people from multiple disciplines, not just Information Technology, engaged in cybersecurity helps create a culture of increased cybersecurity across the organization.

> *Knowing what your clients expect in terms of security is important. For this reason, when the objective is to identify opportunities, your tactical advisory team might include sales, marketing, and customer service advisors. A diverse team can answer questions like:*
>
> - *Do your clients care about the data you collect?*
> - *How do prospective clients determine if your operations are secure?*
> - *Do clients have current or pending regulatory requirements that vendors must meet?*
>
> *When clients value the data being collected you can leverage that by investing in above average security controls. Not only will this reduce your risk, but it builds trust and confidence with your clients, which may allow you to charge a premium.*[1]

This example is just one way to find opportunity within the cyber risk landscape. In business to business settings, which the CSF refers to as Supply Chain Cyber Risk Management, suppliers my find opportunities to land contracts with clients when they can demonstrate a better security posture than their peers.

Similarly, large private entities and government agencies may find that creating *opportunities* for their suppliers is a better alternative to demands and regulations. As illustrated in the next topic for consideration, pressure to comply can inadvertently increase risk.

### Workforce / Supply Chain Risk

With regard to both section 4.3 Cybersecurity Workforce and section 4.4 Cyber Supply Chain Risk Management of the CSF roadmap, please note that there is an inherent risk in having a tight labor pool that is exacerbated when an organization begins to pressure its supply chain to increase its cybersecurity posture. The risk, outlined below, should be considered when developing strategies to increase CSF adoption.

1. *As big companies armor up, attackers turn to less protected small businesses.*
2. *Small businesses cannot afford to compete with big companies for the cybersecurity talent and solutions they need to protect themselves.*

[1] Arnold, Rob (2017).

> *These are circular issues with one begetting the other. In their wake, the demand for affordable solutions will rise dramatically, creating yet another threat. Small businesses desperate to meet the cybersecurity demands of larger clients, government regulations, insurance carriers, and lending institutions are going to become victims once again. Adversaries will use this opportunity to sell cheap software and services that are subsidized by selling data and secrets out the back door and give them a toehold in the supply chain of larger organizations.*[2]

Solving the workforce issue while creating more demand in the supply chain is not an easy balance to achieve and maintain. Any regulations placed on downstream suppliers should consider the effect of doing so when talent is scarce. The roll out issues of SP 800-171 within the DoD supply chain may be a good place to begin this research.

**Engaging Senior Leadership**

The objective of engaging senior management and board members in the governance of cyber risk is paramount. Unfortunately, the technical depth and breadth necessary to cover such a broad and complex topic can make the CSF intimidating. Complaints that it is too complex for executive use likely stems from the fact that the CSF does not clearly delineate what is strategic and what is tactical.

> ***Strategy*** *refers to high-level planning and management. Setting goals and managing toward them with clear budgets and priorities is a strategic duty, but there are others. Determining an acceptable level of risk, encouraging employees to take cybersecurity seriously, managing contractual liability, and protecting the reputation of the company are a few examples. Other roles and duties will emerge in later chapters as we cover different aspects of managing cyber risk.*
>
> ***Tactical*** *refers to using a special skill, or competence, to dive deeply into a specific area of concern. Tactical solutions are the building blocks with which a strategic plan is implemented each playing a specific function within a larger strategy. Tactical cybersecurity functions include IT, legal, accounting, insurance, and other specialties that can be applied to reduce risk. Each plays a role in preventing attacks and reducing the impact of adverse events.*[3]

[2] https://smallbusiness.house.gov/uploadedfiles/11-15-17_arnold_testimony.pdf
[3] Arnold, Rob (2017). *Cybersecurity: A Business Solution*. p. 12. ISBN 978-0692944158.

One place that NIST does begin to make this separation is in SP 800-39 where "tiers" are defined as:

> *To integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.*

Unfortunately, the current version of SP 800-39 is dismissive of Tier 1 risk assessments yet these are the very types of cyber risk assessments that connect the boardroom and strategic mission to cybersecurity. Tiers 2 & 3 are presented as different managerial levels of the tactical implementation. Also, while very large organizations may benefit from the three tiers described in the NIST SP 800-39 & SP 800-30, small and medium companies are rarely complex enough to have three distinct management strata. In small companies, the owner/executive often wears both the strategic and implementation hats. Consolidating the three tiers into two might help make the concepts more friendly to small and medium business.

Also, please note that the CSF uses the term "tier" to mean something completely different than SP 800-39 & SP 800-30. In the CSF tiers refer to maturity levels, not organizational strata. Please consider using a different terminology when SP 800-39 is next revised. Perhaps the strategic/tactical terms would make sense, or stick with "levels" since that is already in the definition of each 800-39 tier.

One final suggestion, while on the topic of terminology. It would be helpful if NIST would create and apply consistent definitions to differentiate between risk assessments, audits, and vulnerability assessments.[4] The framework and its supporting documents seem to use the terms interchangeably, which can frustrate implementation efforts.

**Explicitly Include Cyber Incidents**

It is wonderful to see an increased emphasis on the importance of data sharing. Please consider including cyber *incident* reporting along side the call for sharing cyber intelligence.

[4] https://danielmiessler.com/study/security-assessment-types/ and https://threatsketch.com/3-types-cyber-security-assessments/

1. *Incident reporting refers to an after the fact report of companies that were attacked. It includes victim demographics, methods of attack, and losses incurred.*

2. *Cyber Intelligence generally refers to leading indicators of attack, and examples include newly discovered software vulnerabilities, suspicious activity, signatures of malicious software, and information about adversaries such as new capabilities.*[5]

Having a good source of quality data on incident rates and impact plays a key role in developing the quantitative risk assessments and insurance products that senior executives need. Throughout the roadmap there are references to the need for economic measures of risk, more engagement of senior management, and better strategic decision making tools. Nearly all of these objectives are served by having quality incident data that, like neighborhood crime statistics, give people the data they need to understand their risk and make good decisions.

**How Can We Help?**

Threat Sketch is working on many of the problems outlined on the CSF roadmap. For example, the Department of Homeland Security and the National Institute for Hometown Security are working with us to develop cyber risk management tools for the nonprofit sector. The design of these tools leverages what we have learned works and does not work with small and medium businesses. If your team has interest in collaborating with us on the topic of strategic cyber risk management or how to best approach small and medium businesses, please reach out.

Sincerely,

Rob Arnold
Founder & CEO
Thereat Sketch

[5] https://smallbusiness.house.gov/uploadedfiles/11-15-17_arnold_testimony.pdf