NIST Cybersecurity Framework 2.0. RFI

Evaluating and Improving Cybersecurity Resources:

The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Submitted By

DVMS Institute LLC

www.dvmsinstitute.com

April 2022

What has changed?

We should first look back at the imperative that prompted then-President Obama to issue the Executive Order that led to creating the NIST Cybersecurity Framework. There was a persistent threat of cybersecurity attacks on the nation's critical infrastructure. The Framework provides an easily adoptable risk-based framework with suitable guidance for most organizations in each critical infrastructure sector. Later, federal and state public sector agencies were urged to adopt the Framework following high-profile cyber incidents.

Flash forward to 2022; what's changed? The US adoption of the Framework within the critical infrastructure sectors has been voluntary up to this point. According to the GAO's last report, it has become required within the federal sector, but adoption is far behind the curve. Over the intervening years, the threat landscape has expanded as state-sponsored and state-supported attacks have increased. High-profile attacks make headline newsweekly. It's estimated that only about 30% of critical infrastructure sector organizations have or are adopting the Framework.

However, new imperatives have emerged as legislation and regulations have started holding the board and the organization's executive staff personally accountable for a cybersecurity breach absent reasonable cybersecurity precautions. This raises two questions; 1) what has caused the low level of adoption among the critical sector and governmental agencies, and 2) what must be done to make the Framework easier to adopt, adapt, and implement?

What's missing?

The Framework speaks explicitly about the creation and preservation of value. A recent Micro Trend survey noted that 90% of managers surveyed viewed cybersecurity as an impediment to achieving their business goals. At the top level of organizations, there seems to be a disconnect between creating value and the need to preserve it. While organizational culture is outside the Framework's scope, it provides the context in which the Framework seeks adoption. The Framework lacks guidance around governance, which provides the organizational objectives and policies to create or improve capabilities, and assurance, which proves the execution of the strategic policies.

Suppose the adopting organization internalizes the need to create and protect value. In that case, objectives and policies that flow out of that paradigm shift will cause it to self-organize to achieve those goals. The lack of governance and assurance within the Framework disconnects the imperative of creating and protecting value with the organizational capabilities necessary to achieve that goal.

While the Framework does an excellent job addressing what the Framework does and why it's needed, it provides no pathway to "how" an organization adopts the Framework and adapts and implements the cybersecurity controls of its informative references. The sheer number of controls for small to medium-sized organizations freezes them into inaction. To them, the Framework is the "elephant," and they don't know how to eat it. There is no practical guidance in the Framework that prepares an adopting organization for what's ahead as it tries to get ready, to get going. It lacks guidance on "how" to do "what" is needed. There should be no assumption within the Framework that the adopting organization has the underlying organizational capabilities required to integrate the necessary cybersecurity controls with their existing capabilities or know where to start.

An adopting organization also faces another challenge of what to implement when and in what order, if any. There is no guidance within the Framework for approaching the adaption of cybersecurity controls to the organization's needs and the order of implementation. Nor does the Framework offer guidance on what underlying organizational capabilities are required to implement new or improved existing controls.

What's needed?

Frameworks are descriptive, not prescriptive. What the Framework lacks are perspective and context.

Cybersecurity is not an IT or a business problem; it's an opportunity for organizations to integrate the protection of the value it creates as an aspect of quality. Cybersecurity is not a system of technological siloes but part of a system of systems that creates and protects the delivery of value to the stakeholders. That is why adding governance and assurance is essential to the Framework update and its value to the adopting organization. This makes the Framework more relevant across the organization's digital assets irrespective of their size, complexity, and connectedness.

Guidance is explicitly needed to address the minimum capability the organization must have to successfully adapt the Framework's guidance for implementing or improving cybersecurity capabilities. Many organizations that make up the critical infrastructure are small to medium-sized organizations with immature organizational capabilities. While the Framework can't assume an organization's risk appetite, it would be helpful to either have or reference a capability maturity model such as C2M2 as a simple and usable model that provides the adopting organization with demonstrable measures they can use.

The COSO Enterprise Risk Management Framework provides an excellent, principle-based approach to integrating cyber risk in the organization's overall enterprise risk management strategy. It also calls for the protection of value created. It acts to encapsulate the organizational imperative to create, protect, and deliver value to its stakeholders. An ERM provides the board/executive level imperative to adopt the Framework as a cyber risk mitigation strategy as part of larger overall governance and assurance of enterprise risk. The importance of mentioning it here is that the Framework must seek to elevate its adoption as a technical solution to cybersecurity to a business opportunity to create, protect and deliver value to its stakeholders.

Summary

The Framework needs to provide value in the larger context of enterprise risk management and seek to convey the imperative that value created must be protected. This requires adding guidance that includes governance and assurance. Adopting organizations need a pathway from "what & why" to "what & how" and "what & how much." Part of that may be external references that provide a more holistic or systems view of cybersecurity in a larger context.

About the DVMS Institute

The DVMS Institute's mission is to teach organizations of any size to leverage the NIST Cybersecurity Framework and existing business systems to become an adaptive, cyber-resilient digital organizations.

The Institute's vision is to create a global association of cybersecurity risk management professionals focused on building adaptive, cyber-resilient digital businesses and becoming active contributors to the NIST Cybersecurity Framework and the Institute's DVMS-CPD model and programs.