CSF – Next poor Risk model?

NIST has released its final version of its Cybersecurity Framework (CSF) v1.1. In the CSF, the framework outlines the concept of "profile". The concept of a profile in the context of the framework, I believe, is a mechanism to help "roadmap" and measure success in applying the CSF. However, I think the unintended consequence is a shift of poor risk-based practices from NIST's Risk Management Framework (RMF) to CSF Profiles. This will result in no improvement in Cybersecurity because of the renaming of the poorly implemented risk-based model under a new name. So, what do I mean? Let's look closer.

NIST CSF defines its profile as:

> *The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs. Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations. This Framework does not prescribe Profile templates, allowing for flexibility in implementation. Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps to fulfill a given Category or Subcategory can contribute to the roadmap described above. Prioritizing the mitigation of gaps is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge the resources needed (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. Furthermore, the Framework is a risk-based approach where the applicability and fulfillment of a given Subcategory is subject to the Profile's scope.*

I believe the intent of this definition is an agreed upon description of the risk according to the entire organization. This means the mission, the support, the IT, the security assessors all agree on a single description of risk to the organization (risk profile). This profile should describe the risk

CSF – Next poor Risk model?

aligned with the categories and sub-categories of the Cybersecurity Framework. That allows everyone to communicate in common vernacular.

The logical next step, and I believe the intent of the CSF, is to then have the security practitioners take the mappings to CSF to outline the required security controls to address the risk based on the selected profile. The problem here is the human bias that is introduced in the decision process of choosing the security controls. The Cybersecurity Framework's controls are well defined. So being COMPLIANT is straight forward. The profile has become an easier way to implement bias into the CSF. However, just implementing self-selected controls through the profile identification, does NOT mean you have selected all the right controls, nor does it mean you have achieved a healthy state of Cybersecurity posture. Additionally, because of the CSF's simplicity and appeal to bring together disparate parts of the organization (security, mission, IT, etc.), I believe that the profile construct will be misused under the guise of implementing the CSF and replace the misuse of RMF as the new way to do poor risk management. This approach, simplistic and human biased, will set organizations up to continue the broken model of de-selecting controls wittingly, unwittingly, knowingly or unknowingly that deteriorate Cybersecurity posture. RMF isn't working today. Why? We, as organizations, continue to use "risk-based decisions" to mean less and less known security for convenience or because we don't understand the risk. We use arbitrary baselines and "best practices" to inform us what to do rather than a true understanding and awareness designed to increase Cybersecurity resiliency. Again, how well is this working? As evidenced by the eve-increasing penetrations, hacks, breaches and compromises? Not well.

The worst-case scenario, in my opinion, is if CSF profiles are used as baselines. As, I have said before a baseline is nothing but an auditors opinion against a chosen set of controls/best practices at a point in time. It has very little use, except for auditing and short cutting real Cybersecurity.

Since there are many industries trying to publish CSF Profiles for their respective industries. Again, if the purpose of a CSF profile is for an organization to articulate and map risk to the CSF, how can an industry group outline what needs to be done for a specific organization? We are sliding into bad learned habits of "just give me a baseline to achieve and I'm good" without understanding Cybersecurity Awareness and Resiliency. This is just an easier way to continue the bad habits we have learned in RMF. It is a shame that the CSF explanation of the purpose of Profiles isn't clear enough to prevent this misuse.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us