WHAT DOES NIST CYBERSECURITY FRAMEWORK V2.0 MEAN FOR THE MAINFRAME?

On February 26, 2024, the U.S. National Institute of Standards and Technology (NIST) finalized the first major update to its Cybersecurity Framework since its inception in 2014. With the original framework being used internationally and translated into 13 languages, version 2.0 is expected to have a big impact. Those already familiar with the original know it is comprised of five key areas: Identify, Protect, Detect, Respond, and Recover. Version 2.0 now has a sixth function that is applicable to all of the original five pillars: Govern. Throughout this blog, I will refer to Cybersecurity Framework 2.0 as "CSF 2.0."

Figure 1. NIST v2.0

What is the purpose of the Govern function?

Govern will establish and then continue to monitor an organization's cyber risk management strategy, expectations, and policy.

It is broken down into the following categories:

- Organizational context
- Risk management strategy
- Cybersecurity supply chain risk management
- Roles, responsibilities, and authorities
- Policies, processes, and procedures
- Oversight

Is the Govern addition the only change?

The short answer is "no." While the five functions stay largely the same, there are other new changes, as follows:

- **Implementation examples:** CSF 2.0 now includes examples of how to implement the controls. While it is quite prescriptive, it is not granular. An example here might be the implementation of multi-factor authentication (MFA), but not which MFA factors should be used; that would still be at the discretion of the internal team.
- **Clarity:** While the original framework was digestible, it still used technical language. CSF 2.0 simplifies things, which will hopefully help all stakeholders better understand the controls.
- **Govern function:** Yes, the Govern function is new, however, a lot of it has come from re-

shaping previous controls in the original framework.

- **Updated Respond and Recover functions:** Respond and Recover have gone through a big overhaul, with notable changes around communication and testing.
- **Profiles:** Profiles and community profiles did exist in CSF1.1, however they now have been re-vamped for CSF 2.0. The community can now provide examples of how CSF 2.0 can be applied to certain use cases such as financial, car manufacturing, etc. NIST also provides templates for organizational profiles, allowing side-by-side comparison for gap analysis.

What do mainframe security teams need to do?

Some good news: If you implemented CSF 1.1, all that hard work will not have been in vain and will map into CSF 2.0. There will be gaps that require some changes to be made, so the first thing to do is a gap analysis. NIST provides a host of resources and help in this area. This gives you an opportunity to bring all stakeholders together and, with the new simplified language, should make the process more streamlined than before. Bolstering the Respond and Recover functions could be possible pain points, however all of this leads to a tighter security posture.

Summary

Six years after the introduction of CSF 1.1, we have received a major update from NIST. SCF 2.0 does look quite different from v1.1, but a lot of the work has already been done if you have CSF 1.1 in place. A gap analysis is going to be the first step for any organization. If investment in Respond and Recover is needed, this will not only help you prepare for other regulations, such as the EU's Digital Operational Resilience Act (DORA), but also improve your organization's overall security posture. As far as I can see, everybody wins!