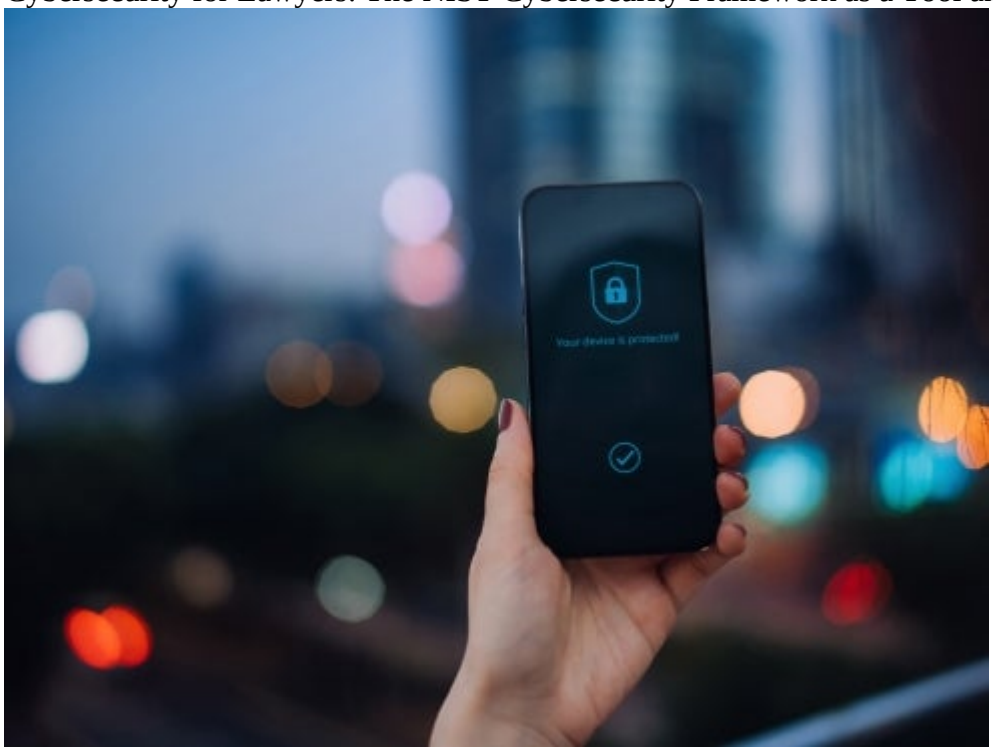
Blogs
September 25, 2024
Cybersecurity for Lawyers: The NIST Cybersecurity Framework as a Tool and Reference



In this post in our series on basic cybersecurity concepts for lawyers (see ***here*** and ***here*** for prior posts), we delve into the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, which is a "taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks."[1]

The CSF, which is a voluntary government resource, boils down to a list of high-level assessment questions that can help any organization (industry, government, academia, nonprofit) assess and improve its cybersecurity. For many organizations, the CSF can be a useful tool and resource for the simple reason that it facilitates understanding of what questions the organization can ask to get a sense of the robustness of its cybersecurity program and also provides examples of how to address those questions. Accordingly, the CSF can be used not only as an assessment tool but as a reference or guide for identifying some options to address common issues.

CSF: Understanding the Framework

If we were to compare cybersecurity to one's overall physical health, the CSF is like a physical health testing profile that measures things such as resting heart rate, cholesterol, the ability to do x number of pull-ups, and the ability to run at a pace for a period of time as an overall proxy for one's physical health. It does not mandate that you do any specific exercises, diets, or any sort of routine but provides you with a useful baseline to understand where you are at a point in time and ways to advance in a way that works best for you. For someone who wants to improve their score on that testing profile—let's say their ability to do pull-ups—they likely have a few different options, such as increased exercise for muscle gain, changes to diet for weight loss, or a combination of the two. However, the ideal plan to increase one's score would certainly vary from one person to the next. The value of the test is that it allows one to figure out where they want to improve so they can focus their efforts effectively and achieve a self-defined "personal best." The CSF works in the same way by "a taxonomy of high-level cybersecurity outcomes that can be used by any organization … to better understand, assess, prioritize, and communicate its cybersecurity efforts," but at the same time, it "does not prescribe how outcomes should be

achieved."[2]

The Goal Is Achieving a "Personal Best" for Security

At its most basic level, the CSF is a set of 96 statements that describe various cybersecurity outcomes (e.g., the organization has a policy in place to identify all contractual reporting obligations associated with cybersecurity incidents) grouped into the following six categories known as the "CSF Core": (1) Govern; (2) Identify; (3) Protect; (4) Detect; (5) Respond; and (6) Recover. In other words, the core inputs are a list of 96 self-assessment statements. What makes the CSF useful is that the CSF Core questions are meant to provide its users with some confidence that they are, in essence, asking all the right questions. Indeed, the CSF does not itself require a particular level of compliance (i.e., a minimum score) but instead encourages an organization to decide for itself its target "CSF Tier," which amounts to a characterization of "the rigor of an organization's cybersecurity risk governance and management practices." The CSF provides the following four CSF Tiers: (1) Partial (Tier 1); (2) Risk Informed (Tier 2); Repeatable (Tier 3); and Adaptive (Tier 4). A chart with notional definitions for these tiers can be found in Appendix B of the CSF.[3] Note that the CSF asks an organization to select a CSF Tier to aim for but does not advocate a particular tier to be selected.

The Mechanics of a CSF Assessment

To conduct a CSF assessment, an organization walks through the CSF Core assessment statements (or a portion of them, depending on how the assessment is scoped) and notes where there are deltas between the status quo and the organization's desired state. This typically requires discussions with relevant personnel and reference to internal policies, practices, and controls. Where there are gaps between the status quo and the organization's desired state, the organization can look to CSF reference material to understand possible ways to close the gap. Still, of course, the CSF is designed to allow an organization to implement its own solution to the issue because its focus is not on dictating controls but rather, like the health test described above, providing a framework for an organization to assess its cybersecurity against a desired state so the organization can define and hopefully meet its own personal best.

However, for those organizations seeking to see examples of the types of conduct that would support a given outcome, NIST provides potential implementation examples for each of the outcomes, as well as references to other cybersecurity standards (from NIST and elsewhere) that provide or reference practices that relate to a particular outcome.[4] As a result, whether or not an organization is undergoing a CSF assessment, the implementation examples can be a valuable resource to anyone seeking to get a sense of ways to address common cybersecurity issues. For instance, the CSF Core includes the assessment statement that "[l]egal, regulatory, and contractual requirements regarding cybersecurity – including privacy and civil liberties obligations – are understood and managed." In connection with that assessment statement, NIST provides the following implementation examples,[5] which provide a very high-level sense of how an organization could address this issue:

- Ex1: Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation)
- Ex2: Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information
- Ex3: Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements

Accordingly, while the CSF may guide users toward accepted practices, it does not mandate any particular solution to address any of its assessment statements. Instead, it provides a framework for an organization to understand the issue it needs to resolve and a sense of some options for doing so.

*****

The CSF, properly understood, is a list of the questions an organization can ask itself in gauging its cybersecurity program. As a result, it is useful not only as an assessment tool but as a reference or resource for anyone who wants to get a better sense of the types of questions an auditor or regulator might consider when

---

[1] The NIST Cybersecurity Framework (CSF) 2.0 at 1. The CSF was updated to version 2.0 on February 26, 2024.

[2] *Id.* at i.

[3] The NIST Cybersecurity Framework (CSF) 2.0, Appendix B.

[4] CSF 2.0 Informative Reference in the Core contains the implementation examples and references to related cybersecurity standards. The CSF 2.0 Implementation Examples document contains only the implementation examples.

[5] The implementation examples in the NIST-provided examples are not meant to be mutually exclusive. These would be implemented in tandem.

Authors

Explore more in

Data Security Counseling and Breach Response

Related insights

Blog

Cybersecurity for Lawyers: A Series

Blog

Cybersecurity for Lawyers: Open-Source Software Supply Chain Attacks