Jody Miller

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) is guidance informing organizations of any size or in any sector what cybersecurity goals they can aspire to achieve in protecting their assets and assessing cybersecurity risk. The CSF doesn't tell an organization how it will achieve the goal exactly, i.e. it doesn't provide the specific technology or controls required to do the job, it leaves that up to the organization to decide but provides many resources within its guidance.

The CSF provides a way to assess the risks that are relevant to an organization as described through several core functions: Govern, Identify, Protect, Detect, Respond and Recover. Each of these core functions is broken down into categories and subcategories that further help define what type of information or consideration is needed to assess and determine goals for that particular function. As an example from the CSF Implementation Examples document, under Govern the first category is Organizational Context and the first subcategory is GV.OC-01: The organizational mission is understood and informs cybersecurity risk management. An organization will define it's mission as a basis for identifying cybersecurity risks.

An organization can create one or more organizational profiles to scope out the risk for a particular organizational function in a variety of different ways such as one for third party systems and one for user facing systems among others. The organizational profile describes the current posture of the organization as it relates to the CSF functions and can also include target profiles. The target profile, if included, is used to describe where the organization wants to be in terms of cybersecurity. This provides a way to do a gap analysis between current and target states and develop an action plan, which feeds a cycle of continuous improvement. Additionally, one of four tiers can be added to each profile to inform of the stance the organization takes in dealing with the risks: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). Partial would be more information while Adaptive is data fed and continuously updated to address the evolving risk landscape.

Small Business Implementation

Implementing this framework within a small business is highly beneficial in my opinion but often overlooked. In my experience, small businesses aren't really thinking of cybersecurity until something happens since it seems to them that they would never be a target. It's better to start while the company is small and get the right mindset and framework in place that way as growth and risk increases, the company is prepared to deal with incidents. The first

step is identifying what kind of risk the company might face. In my experience, small businesses often receive phishing emails and some have led to successful exfiltration of data and/or money in some cases.

The CSF Small Business Quick Start Guide would have been incredibly useful in these scenarios to guide creation of cybersecurity policy on the appropriate scale. First, having a more defined definition of responsibilities between Managed Service Providers (MSPs), if applicable, and the business is extremely important as it is a shared responsibility and dependent on the services contractually agreed to with the MSP. The CSF Small Business Quick Guide is a good place to start from and following its guidance helps ensure everyone is clear on responsibilities, knows their role, and helps identify gaps that may not be discovered until an incident occurs.

Answering the questions from the Govern function provided in the guide would inform better decisions. For example, what cybersecurity risks may prevent us from achieving this mission? Phishing would be the number one direct issue beyond something like a DDOS or other attack on actual networks or devices. The acceptable use policy that is mentioned on the same Govern slide is also important and having that in place along with appropriate training for new employees and on a recurring basis could help prevent the type of attacks that small businesses face.

Under the Identify function, the table example for assets is something that should be used in a small business and is a good place to start so that everything is documented in one place. In the Protect function, much of this would be done in conjunction with a MSP, if applicable, whose role typically includes items like patching and updating of systems and backups along with disk encryption. Having regular communication with employees regarding recognizing attacks is a key point here since the human risk factor is generally the most important risk to contain.

The Detect and Respond function actions are also highly dependent on an MSP if providing antivirus on business devices, monitored computers/networks, providing incident response and after-action reporting. The key here is definition of responsibilities, employee awareness campaigns for signs of intrusion, and a communication plan for internal and external stakeholders. And finally, the Recover function, defining the responsibility and then the post-incident report in collaboration with the MSP to understand what happened. Outlining it as it relates to the CSF framework and knowing this is an expectation has a lot of value.

Overall, the CSF Small Business Reference Guide is a great resource and I would certainly recommend its use in retrospect, having dealt with some of these issues firsthand. The

document breaks down the important aspects for a smaller business where the larger guide might be overwhelming and harder to fine tune.