tracesecurity
Compliance, simplified.

White Paper

A Guide to Successfully Implementing the NIST Cybersecurity Framework

Jerry Beasley

CISM and TraceSecurity Information Security Analyst

Executive Summary

By the nature of their work, information security analysts see the inherent weaknesses and growing threats to information systems as they are engaged to test the security controls of organizations via penetration tests, physical security exercises, and in-depth vulnerability assessments. The rest of the world need only read the headlines to learn of major cybersecurity breaches affecting millions of individuals across the U.S. and internationally. This recognition of very real threats was the progenitor of actions by the U.S. Federal Government to establish a common framework to manage and implement cybersecurity defense.

To address the growing threat, on February 12, 2013, the President of the United States issued Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity." The purpose of the EO was to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The order provided a mandate to establish a voluntary common framework for cybersecurity defense.

In response to this mandate, the National Institute of Standards and Technology (NIST) was tasked with development of the Framework for Improving Critical Infrastructure Cybersecurity. This is more commonly known as the Cybersecurity Framework (CF). The CF consists of standards, guidelines, and practices to promote the protection of critical infrastructure. Much of the CF is derived from NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", but the CF also encompasses many other guidelines and frameworks.

This white paper provides background information on the CF guidance and explains how organizations should use the framework to better manage and reduce cybersecurity risk.

Identifying the Need for Cybersecurity Guidance

Despite increasing defensive efforts, the number of successful cyber attacks continues to rise. According to a 2015 Symantec report, the number of sensitive data breaches increased by 23 percent in 2014. Malicious attackers were responsible for the majority of these breaches, which were not limited to high profile companies and organizations. According to Symantec, 60 percent of all targeted attacks struck small- and medium-sized organizations.

The 2013 EO directed at improving cybersecurity defense was defined as being applicable to "critical infrastructure." But what does critical infrastructure refer to? The EO defined it as follows: "...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Before you breathe a collective sigh of relief, think about what this means. Who has an impact on national security? Based on the definition, one could certainly think of utility companies, financial institutions, healthcare organizations, emergency response agencies, and law enforcement, but what about commercial entities, research institutions, and the myriad of organizations that interface with these types of institutions? One thing is clear, it is difficult to define which organizations are critical and which are not. This is due to one nagging fact. We are interconnected. Therefore, when considering the interconnected Internet, a risk to one is truly a risk to all.

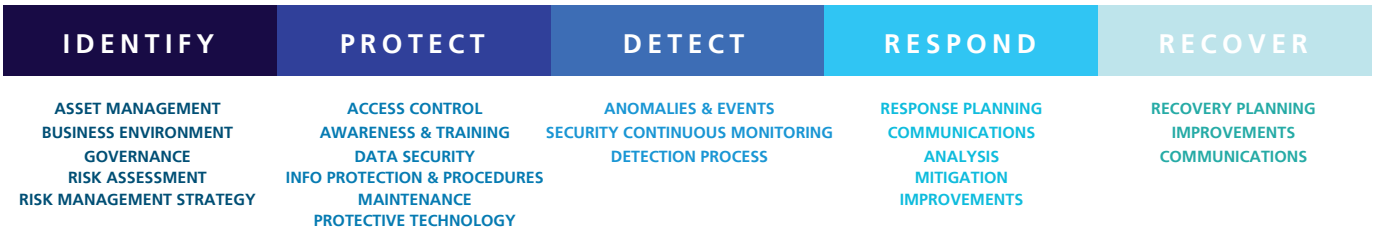
The CF was designed to be technology neutral and industry agnostic. Since its inception, the CF has been adopted in many industries across the U.S. and internationally. The elements of the framework core should be applicable to any organization that creates, processes, accesses, or stores sensitive information. In fact, some industry regulatory bodies have published additional implementation guidance supporting the framework.

For example, in 2015, the Federal Financial Institutions Examination Council (FFIEC) issued implementation guidance in the form of the FFIEC Cybersecurity Assessment Tool. The assessment tool provides financial institutions a means to analyze their inherent risk and the relative maturity of their cybersecurity programs. While not a replacement for an institutional framework, this industry tool provides a means for organizational leaders to obtain a high-level view of their overall risk and cybersecurity program implementation. Establishing an institutional framework takes time, but with the help of the CF, an organization can build their own roadmap for achieving an appropriate level of cyber readiness.

The Primary Components of the Framework

The NIST CF consists of three primary elements: implementation guidance, the framework core, and a framework profile. NIST provides guidance for implementation that includes a cyclic approach to evaluate risks, identify gaps in program implementation, and implement action plans to address any discovered gaps. Because risk management is the foundation of a cybersecurity program, the CF guidance emphasizes the integration of the CF into an organization's overall risk management program.

The framework core is the meat of the CF and provides a common baseline of cybersecurity activities applicable across different industries and industry sectors. The framework core is aligned to the common cybersecurity functions of threat identification, protection mechanisms, threat detection, incident response, and incident recovery. The following is a visual representation of the common cybersecurity functions.



Source: National Institute of Standards and Technology

For each cybersecurity function, categories of general activities are identified that are commonly used to implement a particular function. The following is a visual representation of the categories.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Info Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications

Source: National Institute of Standards and Technology

For each category of activity, subcategories are also defined that provide the recommended implementation steps for each category. However, realizing that organizations have unique needs, NIST provides the flexibility to tailor the subcategory controls to meet individual business requirements. For instance, omitting a subcategory that is not applicable to an organization or adding additional subcategories to address unique threats in an organization.

Great planners understand that it is important to know both where you are at today, as well as where you are going. The difference between the two can provide a map for achieving your goals. Enter the CF Profile. The purpose of the framework profile is to document the current status of an organization, or for a new program, the objective status of the organization. It is essentially a snapshot of an organization's prescribed and implemented controls. This snapshot is compared to the objective framework to identify any gaps, and the gaps then drive plans to address any deficiencies in the program.

The final element of the CF is the definition of "implementation tiers". These tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework. This provides a common language and criteria for determining an organization's progress at implementing the CF. However, it is important to realize that the implementation tiers are not intended to be a formal assessment or certification program. Instead, they are designed to be a tool for organizational leaders to evaluate their progress at implementing the framework.

Scenarios for Framework Adoption

At this point, you have hopefully garnered support from your organizational leadership and are ready to move forward with implementation of the framework. Where to start? Well, that depends on the current state of your organization's cybersecurity program. Let's consider two scenarios: integration into an existing program and establishment of a new program.

The CF is intended to complement, not replace, an organization's risk management process and cybersecurity program. As a result, there is no need for organizations with an existing cybersecurity program to recreate their programs from scratch. These organizations may continue using current processes and compare their existing cybersecurity programs to the CF in order to identify opportunities for improvement. Where warranted, the elements of the CF not already addressed can be incorporated into existing programs.

Alternatively, organizations without an existing cybersecurity program can use the Framework as a model to establish one. As illustrated previously, the CF is divided into cybersecurity functions, function categories, and subcategories. So a good place to start when establishing a new program is with the high-level functions of identification, protection, detection, response, and recovery. For each function, the organization should develop a high-level strategy for meeting the function objective. For example, given the cybersecurity function of "identification", how does the organization envision implementation? Will it use internal resources, contracted resources, manual processes or automation? How will the function be managed? What is the required implementation timeline? What general tools, systems, or service agreements will be required? Any strategy will require securing management buy-in and dedication of the resources required.

Given the approved high-level strategies to address each cybersecurity function, the organization must now drill down into the categories of function implementation. For example, the identification function is divided into the categories including, but not limited to, Asset Management, Governance, and Risk Management. The organization needs to identify who will be responsible for each category and what those responsibilities should be. They should also ask what resources will be at their disposal and what foundational policies will govern implementation. The answers to these questions may translate into duty descriptions, committee charters, organization charts, etc. that support the establishment of the program.

Finally, with an established team, the organization can begin addressing the subcategories that equate to the implementation steps for each activity. This is where CF subcategories are translated into action plans. The level of detail is higher at this stage and attempts to document the specific steps, as well as who, when, where, and what resources are required for each step. At this point, we have defined most of the essential elements of the framework. The functions, roles and responsibilities, categories of activities and specific activity steps have been defined. We are done, right? Well, not quite. The last piece of the puzzle is still missing.

Measuring Successful Implementation

When establishing any process, a measurement of success must be defined or at the very least a measure of whether or not the process is working as designed. Ultimately, the framework is not complete without defining the means of measurement. As indicated in the NIST CF guidance, one essential measurement is risk. A risk assessment identifies the risk remaining after implementation of the framework and associated controls. As part of a cyclic process, the organization should conduct risk assessments identifying the information assets protected, the threats impacting those assets, and the mitigating controls in place to reduce the impact or likelihood of the threats. The residual risk that remains must be accepted by the organization, avoided, or further mitigated by the implementation of additional or enhanced existing security controls. In this way, risk management provides the foundation of the framework and a means to identify elements of the framework that should be strengthened.

The organization may also choose to perform additional measurements to facilitate regulatory compliance or to provide additional metrics for measuring success. These can include, but are not limited to, formal audits, gap analyses, technical testing, and contingency exercises. Regardless of the specific mix of testing and assessment, the ultimate goal is to improve the organization's cybersecurity defenses. Establishing a feedback loop helps ensure that all lessons learned from regular tests and exercises are incorporated into future improvement plans.

Conclusion: Effective Cybersecurity Risk Management

Cybersecurity threats continue to grow and affect all organizations. The NIST CF was established to provide a common framework to strengthen cybersecurity defenses across critical infrastructure in all industries and organizations.

While framework implementation is voluntary, use of the framework is gaining momentum across multiple industries. Some industries are providing additional implementation guidance, further cementing the framework in these industries. The CF may be used as a gap analysis tool for existing programs, overlaid with existing programs or serve as a model for establishing new cybersecurity programs. The CF subcategories map to the defined controls of most other standards and models to provide the glue that binds the best of those sources into a single framework.

The CF is structured in a way that facilitates a modular approach to implementation, and organizations are encouraged to add additional activity subcategories (steps, controls) to meet the unique needs of their operating environment. Finally, the CF is intended to augment, rather than replace, an organization's existing risk management program, while the risk assessment process can be used as a tool to measure CF effectiveness.

The most successful cybersecurity programs are those that don't simply rely on technical controls but clearly define a framework to address each of the essential cybersecurity functions: threat identification, protection mechanisms, threat detection, incident response, and incident recovery. Combined with an ongoing risk management program, the CF can help build a strong foundation for any cybersecurity program.

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.