RESOURCE CENTER

What is the NIST Cybersecurity Framework? The Ultimate Guide

Get the full interactive view at
https://bitwarden.com/resources/nist-cybersecurity-framework/

bitwarden

History of NIST

The National Institute of Standards and Technology (NIST) provides guidance and best practices for organizations to follow, in order to help businesses, non-profits, and other private-sector institutions to improve cybersecurity risk management. NIST is part of the U.S. Department of Commerce, and one of the nation's oldest (physical) science laboratories.

Back in 2013, the President issued Executive Order 13636 that stated:

> **"It is the policy of the United States 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."**

This Executive Order established certain requirements that NIST applied to their cybersecurity framework, including:

- Identify security standards and guidelines applicable across sectors of critical infrastructure.
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach.
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk.
- Enable technical innovation and account for organizational differences.
- Provide guidance that is technology-neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services.
- Include guidance for measuring the performance of implementing the Cybersecurity Framework.
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.

Why has this become so important?

Put simply, increasing cybersecurity threats affect businesses and other organizations daily. Without a single source of truth, it would be almost impossible for businesses to develop a thorough, effective framework to help them implement effective measures for mitigating security risks. That's why the NIST Cybersecurity Framework has become so crucial for businesses; it encourages efficient, innovative, and resilient solutions to maintain security.

Table of Contents

What is the NIST Cybersecurity Framework?

Essentially, the NIST Cybersecurity Framework helps organizations of all types to better understand, manage, and reduce cybersecurity risks. The end result of following this guidance is better protection of networks and data. The NIST Cybersecurity Framework is broken down in such a way that any business or organization could implement it to better understand where to focus time and resources for improved cybersecurity protection. It's all about empowering businesses to be more effective at protecting their data, their customer's data, their networks, and their employees.

Although the NIST Cybersecurity Framework was developed by an organization within the United States, it was created with the idea of global adoption. To that end, it's been translated into many languages and adopted by governments, businesses, and organizations around the world.

Since NIST Cybersecurity Framework 1.1, many organizations and governments have successfully adopted the framework, including:

- Saudi Aramco
- Government of Bermuda
- Israel National Cyber Directorate
- Cimpress-FAIR
- Multi-State - Information Sharing and Analysis Center
- University of Kansas Medical Center
- University of Pittsburgh
- ISACA
- Japanese Cross-Sector Forum
- University of Chicago
- Lower Colorado River Authority
- Optic Cyber Solutions

The latest version of the NIST Cybersecurity Framework (CSF) is geared for audiences, industry sectors, and organizations of all types and sizes; from small schools and nonprofits to enterprise corporations. The framework was designed so that any organization, regardless of cybersecurity sophistication, can benefit from the information it presents.

According to NIST Director and Under Secretary of Commerce for Standards and Technology, Laurie E. Locascio:

> "The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats… CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization's cybersecurity needs change and its capabilities evolve."

Exploring the history of the NIST Cybersecurity Framework

The latest evolution of the NIST Cybersecurity Framework also goes beyond focusing on critical infrastructure and encompasses all organizations (of all sizes) within any sector.

When the NIST Cybersecurity Framework was created, the goal was about ongoing engagement with stakeholders in government, industry, and academia. In order to create this framework, NIST used outreach and workshops across the country, as well as a Request For Information (RFI) and a Request For Comment (RFC). Their initial goal was threefold:

- Identify existing cybersecurity standards, guidelines, frameworks, and best practices.
- Specify high-priority gaps.
- Develop action plans to address those gaps.

The comment period for information gathering ended on April 8, 2013, and NIST received over 270 responses to the Request For Information. From those responses, NIST developed the agenda for their first Cybersecurity Framework workshop, which took place in Washington DC with the goal of gathering interest, raising awareness, and providing insight into the collaborative development process. The topics of the workshop included the Executive Order, the goals for the development, and reaffirming the process that would be used to develop the framework.

The second workshop took place between May 29-31, 2013 and was held at Carnegie Mellon University with an agenda that was based on the analysis of the initial RFI. The goals were to further define and clarify the information they'd received and encourage debate across several security-based topics. After this workshop concluded, NIST analyzed the information they'd gathered, and created summaries that were shared with the industries and used to create the initial draft of the Cybersecurity Framework.

The first draft of the NIST Cybersecurity Framework was released on July 2, 2013.

NIST held several workshops following the release, geared toward discussing and refining the initial release. On February 12, 2014, version 1.0 of the NIST Cybersecurity Framework was released.

The core functions of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework consists of several core functions, which give a general overview of the best practices. These functions are not intended to be looked upon as procedural steps but, rather, used to address the dynamic nature of cybersecurity risks.

Govern

This function provides outcomes that help inform what an organization can do to prioritize the remaining functions in the context of its mission and stakeholder expectations.

Identify

The identify function calls on the need to develop an organizational understanding of cybersecurity risks to systems, assets, data, and capabilities. This element focuses on the business, so it can prioritize its efforts in a way that's consistent with its risk management strategy.

Protect

This function supports an organization's ability to secure assets, and prevent or lower the likelihood of, and impact incurred by, a cybersecurity event.

Detect

This function enables the timely discovery and analysis of anomalies, indicators of compromise, and other adverse events that indicate a cybersecurity event has or will occur.

Respond

This function helps contain any effects of a cybersecurity incident, covering incident management, analysis, mitigation, reporting, and communication.

Recover

This function focuses on the timely restoration of normal business operations, in order to reduce the effects of a cybersecurity incident, as well as enable the necessary (and appropriate) communication during the recovery.

The ultimate goal of these functions is to offer a high-level, strategic view of how an organization prepares for, reacts to, and recovers from cybersecurity events.

Implementing the NIST Cybersecurity Framework

With a solid understanding of what the NIST Cybersecurity Framework does, and how its evolved, you're probably wondering how best to implement it.

NIST recommends a 7-step approach for implementation, which looks like this:

1. **Prioritize and scope** - Prioritize your organization's objectives and assets that need to be protected.
2. **Orient** - Familiarize yourself and your team with the processes, systems, and components within the scope, as well as the key compliance regulations they must adhere to.
3. **Create a current profile** - Indicate which control outcomes of the framework are already being achieved within your organization, and then create a list of what still needs to be integrated.
4. **Conduct a risk assessment** - Analyze your operational environment to determine the likelihood of cybersecurity events, as well as the impact they could have.
5. **Create a target profile** - Focus on the Cybersecurity Framework Categories and Subcategories assessment to help you describe your desired cybersecurity outcomes.
6. **Determine, analyze, and prioritize gaps** - Determine any cybersecurity gaps that exist in your organization. From this analysis, you can then create a prioritized plan to address those needs.

7. **Implement your action plan** - Take action and implement the plan you've created to address all issues discovered within the previous steps.

One thing to keep in mind is that the framework isn't inflexible. In fact, the framework does offer enough flexibility that it can integrate with your existing security processes. You should see how that works within the seven steps listed above.

Benefits of Adopting the NIST Cybersecurity Framework

Because of how NIST lays out the seven steps for implementing the framework, organizations get an extensive overview of what risks they are susceptible to, how to plan according to those risks, how to improve organization-wide communication and strengthen compliance. The education regarding an organization's weaknesses, and how to mitigate them, is one of the crucial benefits of the NIST Framework.

> According to the Federal Trade Commission, the NIST Framework, "helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data."

NIST understands that every organization is different, and even offers 3 tips to keep your passwords secure (which should be considered universal).

Challenges and considerations in framework adoption

The NIST Cybersecurity Framework can be complex. It's important to fully understand the core functions before you can move on to the seven steps listed above. In order to ensure lasting success, it is critical to encourage a cybersecurity culture within your organization, otherwise, you'll run into resistance to what could be a dramatic change in processes and systems.

Other challenges include:

- Resource constraints - you might not currently have the staff capable of implementing these changes.
- You'll most likely have to spend time customizing the Cybersecurity Framework to better fit your organization.
- Threats are always evolving, which means your security practices will have to keep up.
- You'll want to integrate the Cybersecurity Framework with any existing processes you have in place.
- It may be challenging to encourage stakeholder engagement, which directly relates to fostering a cybersecurity culture that is capable of meeting these demands.

NIST Cybersecurity Framework profiles and tiers

There are four NIST implementation tiers, which are:

- **Tier 1 Partial** - Companies with on-demand or zero security procedures.

- **Tier 2 Risk-informed** - Companies that are aware of the threats they face, and have some policies in place, but lack a coordinated strategy.
- **Tier 3 Repeatable** - Companies with risk management and cybersecurity best practices that have received executive approval. These businesses often measure themselves against competitors, and even work with other organizations to ensure their practices are aligned.
- **Tier 4 Adaptive** - Companies in heavily regulated industries (such as banking and healthcare) that routinely contribute to broad risk awareness.

According to NIST, the Cybersecurity Framework Profile "is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization." These profiles help organizations establish a roadmap to reduce cybersecurity risks.

NIST offers a customizable Cybersecurity Framework Organizational Profile Template, as well as a list of community profiles that can be used.

Updating and evolving with the NIST Framework

Keep in mind, the NIST Cybersecurity Framework is designed to be a living document that depends on regular updates reflecting the ever-changing landscape of cybersecurity and emerging threats. Because of this, it is crucial that organizations stay up-to-date on the latest threats, so the Cybersecurity Framework can evolve to meet current needs and continually improve.

To make sure your organization is capable of evolving with the NIST Cybersecurity Framework, you might consider how to build the best cybersecurity tech stack for your business, as a way to ensure you are capable of leveraging the best technology capable of evolving with the Cybersecurity Framework.

Leveraging Bitwarden for a stronger cybersecurity posture

It should go without saying that security has become one of the single most important areas of focus for organizations. Without robust cybersecurity risk management practices, companies could fall victim to any number of threats in the wild. With the help of the NIST Cybersecurity Framework, along with careful planning/communication, your organization's security could vastly improve. Approach the NIST Cybersecurity Framework thoroughly, follow the 7 steps, and always be ready to update and evolve so your organization will be better protected from cybersecurity risks.

Ready to get started today? Consider adopting a password management solution to start your organization off on the right foot. Check out Bitwarden Business plans, contact sales, and compare plan pricing.