FTP TODAY

WHAT IS NIST?

THE COMPLETE GUIDE TO THE NIST CYBERSECURITY FRAMEWORK

Table of Contents

What is NIST and How Does it Affect My Business?

NIST, or the National Institute of Standards and Technology, is a federal laboratory that, to put it simply, works to improve measurements and standards. Founded in 1901, NIST has a long history of being tasked by the United States government with developing measurements, metrics, and standards for technology in different industries. Because it is a non-regulatory agency, it works closely with commercial industries and other government agencies to establish national measurements to benefit technology development.

So many technologies, from everyday computer chips to major power grids, rely on measurements and standards outlined by NIST. NIST measurements support nanoscale devices so small they're undetectable by the human eye to worldwide communication networks. The breadth of NIST's impact in the technology space is astounding. However, NIST isn't just active in the U.S. It works with similar organizations in different countries to ensure that technologies using NIST standards and measurements are viable on a global scale.

What does NIST have to do with your business? One of NIST's roles is to develop guidelines on how companies can align with Federal Information Security Management Act (FISMA). These standards were created by NIST to be both a set of measures to provide the utmost protection for data and a cost-effective way to ensure companies don't break the bank trying to keep data secure.

Though FISMA guidelines are ideal for government agencies, government contractors, and subcontractors, they can be applied to almost any organization in both the public and private sectors. In fact, more than 30% of U.S. companies use the NIST Cybersecurity Framework as their standard for data protection, and it's projected that by 2020, 50% of companies will be use the Framework as their benchmark for cybersecurity. Because NIST doesn't pertain to a single industry, but a wide range of industries, its regulations can help companies align with other compliance guidelines like HIPAA, SOX, ITAR, and more.

What is the NIST Cybersecurity Framework?

> "The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."- NIST

The NIST Cybersecurity Framework is a set of voluntary standards, guidelines, and processes that companies use to diminish the risk of a cybersecurity threat. Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, was issued in February 2013, and through this order, NIST was directed to partner with key stakeholders to create a framework to address cybersecurity concerns.

NIST worked closely with organizations in the private sector to gain their input and recommendations during a year-long collaborative process. In all, more than 3,000 people from government agencies, academia, and the private sector offered initial suggestions and feedback on the new Cybersecurity Framework. This collaboration allowed numerous voices from a number of industries to provide practical, actionable steps to increase data security.

Is your organization required to use the NIST Cybersecurity Framework? While the framework is designed to be beneficial for companies in terms of cybersecurity protections, use is completely voluntary. You won't face any consequences for not using it, other than being subject to possible data breaches. So, because the Cybersecurity Framework could help be maintain data security, you could avoid some of the common risks associated with a data breach, like lost business or fines related to other regulatory compliance measures.

There are numerous reasons why an organization would adopt the NIST Cybersecurity Framework, the most important of which would be protecting sensitive data. It also works to help prioritize the actions that organizations should take to protect data, ensuring the more critical items are addressed first. The framework is easy to understand, even if you're not a technology expert, and it's an effective way to communicating information about cybersecurity risks to everyone in your organization. Whether your organization already has an extensive set of cybersecurity processes in place, or your business is just starting to assess its cybersecurity needs, the NIST Framework is a perfect set of guidelines that apply to companies in nearly all industries.

How Does the NIST Framework Help Me Better Manage My Cybersecurity Risks?

First and foremost, the NIST Cybersecurity Framework provides a uniform set of standards that can be applied to nearly all companies. In the past, a lack of uniformity at different points of the supply chain – from suppliers to manufacturers to vendors – led to cybersecurity risks for all companies involved. So, while a manufacturer may have enough security measures in place to protect their sensitive data, the vendor receiving the sensitive data may have had minimal security measures in place. Regardless of the efforts on the part of the manufacturer, sensitive files could still be at risk if the vendor is subject to a data breach.

Uniformity in cybersecurity standards gives you greater control over how sensitive data is protected both during and after it is in your possession. Once you commit to using the NIST Cybersecurity Framework, you can also choose to only work with other companies who adhere to these standards. You can clearly communicate your expectations regarding cybersecurity before you hand over sensitive data.

The NIST Cybersecurity Framework gives your company a set of guidelines that are easily prioritized and customizable to best suit the needs of your organization. It can help your organizational leadership and your employees understand the risks of cybersecurity threats and determine the actions you should take to ensure you're not susceptible to these risks.

In addition to preventing cybersecurity incidents, the NIST Framework can help you respond to and contain the impact of an incident if one does occur. Properly detecting, containing, and reporting a cybersecurity incident is a major aspect of the Framework. When you have set

procedures to follow in the event of a data breach, you can respond quickly and reduce risks as much as possible.

The Cybersecurity Framework is a not one-size-fits all set of guidelines. It's not a list of mandated tasks to be completed. It offers flexibility that allows organizations to choose applicable actions and apply them to a degree which will have the greatest impact on their security efforts.

The Framework is also laid out in easy-to-understand terms. Not everyone that is employed by your company has an in-depth knowledge of cybersecurity terms, tool, and activities. The Framework is written in a way that everyone can understand – from your IT director, to your CEO, to your newest intern. It clearly outlines the ways in which your data could be at risk and offers clear, direct actions you can take to mitigate that risk.

Ultimately, the NIST Cybersecurity Framework takes the guesswork out of data security. You don't need to invest time in developing these standards yourself. Instead, you can use a proven and established framework, and only select partners that use it, as well.

What is the NIST Framework Core?

The Framework Core is not a checklist that you can simply complete and forget about. It's a compilation of actions for your organization to complete on an ongoing basis, all concurrent and working together to protect your data. The structure of the Framework is based on desired cybersecurity outcomes your organization should be working toward.

One desired outcome, for example, is that "physical devices and systems within the organization are inventoried." These outcomes act as specific goals companies should strive to meet. They also help to educate stakeholders in your company - leaders and employees alike - on the objectives you're working to achieve. The Framework Core outcomes allow you to easily gauge the success of your efforts and measure the impacts of your actions.

So, let's say your organization inventoried all of your solutions and systems, as recommended by the Framework Core. After completing your inventory, you identified 20 devices that were not password protected and at least one data breach was traced to a non-protected device. After taking action to require password protection, no data breaches were detected on any of your inventoried devices. That is a clear mark of success for your organization.

The Framework Core has an organizational structure that simplifies the application of the Framework to your company. The Framework Core is broken down into five Functions - Identify, Protect, Detect, Respond, and Recover. These Functions are high-level groupings of cybersecurity activities. Think of them as the five general classifications that all cybersecurity activities will fall under. We'll take a closer look at these specific categories in a later section.

Now to the NIST Framework Core, the meat of the NIST Cybersecurity Framework. These are the specific objectives and recommended actions your organization should take to promote cybersecurity.

The five Functions of the Framework Core are broken up into multiple Categories. These Categories address specific activities under each Function, like “Asset Management” or “Identity Management and Access Control”. These Categories are broken down even further into Subcategories focused on specific activities that contribute to securing the desired outcome of the Functions.

Let’s look at a specific example.

- **Function** - Identify
    - **Category** - Asset Management
        - **Subcategory** - Physical devices and systems within the organization are inventoried.

The **Function - Identify -** pertains to identifying and categorizing all systems and solutions your company uses that could house or transfer sensitive data. As part of the Identify Function, the category of Asset Management contains a number of actions you need to take, including inventorying your physical devices and systems.

In addition to Functions, Categories, and Subcategories, the Framework Core also includes Informative References. These references are specific sections of recommended actions that provide instruction on how to achieve the desired outcome of each Subcategory. While these references are illustrative of key actions to take, they are not exhaustive. They act to supplement the Subcategory objectives.

The Framework Core is essentially a well organized set of steps that provide a methodology and process for protecting your data and setting cybersecurity standards in your organization. Remember, the Cybersecurity Framework Core is designed to augment the cybersecurity practices you have already established. It acts as a universal skeleton for the security measures and processes that all organizations should have in place. So, as you explore the Functions below, consider how they relate to your current efforts and how they can supplement your data security measures in the future.

Explore the five Functions of the NIST Cybersecurity Framework, and learn more about adopting these Functions into your own data security processes.

Identify

Identify is the first of the five Functions of the NIST Framework, and it acts as a foundation for all other activities. This Function requires companies to identify all software solutions and systems that play a role in your critical infrastructure. The Identify Function plays two important roles: increases transparency into the solutions that are being used and helps to prioritize actions that protect critical systems first.

In terms of transparency, a common problem that organizations face is shadow IT devices. There are devices that aren't provided or approved by your company, but are still being used. It could refer to an employee accessing their email account through their personal mobile device, or an employee bringing their personal laptop to work instead of using tools provided by their employer.

When you don't know exact which devices are being used and for what purpose, it can be nearly impossible to protect the data stored, accessed, or transferred using these devices. Each unauthorized device that's used could be a potential for a hacker to gain access to your data.

The Identify Function also helps your company identify and prioritize which systems should be protected first. If you identify all systems in your company and determine that secure data is concentrated to solutions in one department, you can take the steps to protect those systems first.

Many companies don't have the time or resources needed to adequately protect their data. That's why prioritization is key. If you can't protect all data at all points, you can at least take steps to protect the most sensitive data.

The following Categories fall under the Identify umbrella:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

The next Framework Function is Protect. This Function is focused on reducing the number of cybersecurity events that could occur within your organization and limiting the impact if one does occur. While many companies may know that they need to protect their data, they may not be aware of what steps they should take. Fortunately, the Protect Function offers a number of actions that will increase your data security.

Companies should be thoroughly aware of the risks associated with a data security breach. Not only can it disrupt your organization's entire operations, but it can also seriously impact the credibility of your business. If a customer trusts you with sensitive financial information, for

example, but that information is stolen during a data security breach, you can understand how that customer would be hesitant to trust you with their data again.

A failure to protect your solutions and systems can also have compliance consequences, too. The recommendations found in the NIST Cybersecurity Framework overlaps in some areas with the mandates of government compliance measures, like HIPAA or ITAR. So, if you fail to protect your data, not only could you lose business, but you could also be subject to fines or even jail time if you're not compliant with government regulations.

The Protect Function encompasses the following Categories of data protection:

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

Despite your best efforts, there's a chance that a data security breach can still occur. It could be due to human error, a common cause of cybersecurity events, or your company could just be the target of a highly sophisticated hacker. Regardless of the cause, the Detect Function outlines how you can develop and implement measures that will help you detect the occurrence of a cybersecurity event.

While it's essential that you are able to detect a cybersecurity threat, detecting these threats in a timely manner is equally important. As the amount of time a cybersecurity event goes unnoticed increases, the threat to your company grows, as well.

You may imagine a data breach happens like they are shown on movie or television, with red alerts and sirens. However, it can take days, months, or even a year to detect a data breach. In fact, more than 25% of data breaches that occurred in 2016 went undetected for more than a month, and 10% of breaches went undetected for more than an entire year. Imagine the amount of information hackers were able to glean during those long stretches of time. Not only was all existing data those companies possessed exposed to a breach, all newly received data was exposed to risk, too.

Here are the Categories of action that fall under the Detect Function:

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

As important as it is to detect cybersecurity events, it's equally important that you respond to them rapidly and effectively. The fourth Function, Respond, offers guidelines on how to develop and implement processes to follow when a cybersecurity event is detected.

These Respond procedures should make it possible for key stakeholders in your company to address and contain any attack with speed. While the other preceding Functions – Identify, Protect, and Detect – are all focused on mitigating the risk of a cybersecurity event, the Respond Function has an enormous impact on the outcome of an event if it occurs. An effective response protocol can contain an event and minimize the amount of damage that occurs. An ineffective response protocol that fails to contain an event could have serious consequences for your organization.

As part of the Respond Function, you will create a plan of action that is communicated to your

team members, ensuring that those responding to incidents, like an employee opening an email with a virus or your systems being accessed by an unapproved international IP address, will know what is expected of them.

The Respond Function features five Categories that help companies build their response plan:

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

The final Function, Recover, involves the steps your company should take in the aftermath of a cybersecurity event. As your organization works through the Recover Function, you will develop and implement a plan for resilience and restoration of any systems or solutions that were impaired by the data breach.

As with some of the previous Functions, successful recovery following a data breach is dependent on rapid response. Consider a scenario in which your data storage server was corrupted by a data breach. When most of your business functionality is reliant on the files stored on that server, all of your operations could be stopped in their tracks, seriously impacting your productivity and your bottom line.

The high-level goal of the Recover Function is to return your business back to normal operations, minimizing the amount of time and data that was lost to the cybersecurity event. While a data

breach can be frustrating and potentially harmful for a company, with an appropriate recovery plan, your operations will return to normal in no time.

Below are the three Categories under Recover. Each one plays a role in returning your operations back to normal following a breach.

- Recovery Planning
- Improvements
- Communications

What are the NIST Framework Implementation Tiers?

The NIST Cybersecurity Framework is not designed to be used by every organization in identical manners. Some large organizations may already have numerous security measures in place that overlap with the Framework, as they are subject to greater risk of data breach. In contrast, small businesses may have fewer channels for potential breaches and are only beginning to build up their data security processes.

Thus, we come to the NIST Cybersecurity Framework Tiers. These Tiers categorize how your company views cybersecurity risks and the processes you have established to mitigate that risk. While many people think of these Tiers as maturity levels, they should be thought of as the categorization the collaboration between your cybersecurity risk management processes and your operational risk management processes. As put by NIST, the four Tiers "describe an increasing degree of rigor and sophistication in cybersecurity risk management practices."

As you evaluate the descriptions below to determine which Tier is most applicable to your business, remember that they are meant to determine the extent to which your cybersecurity measures have been integrated into your business operations, while also identifying whether or not your business requires further integration based on potential risk.

Let's take a closer look at the different Tiers. Which one most closely resembles your organization?

Tier 1 - Partial

Companies in Tier 1 are just beginning their cybersecurity journey. At this point, the organization

may have informal practices in place, but there is little awareness among the employees and stakeholders about these data security practices. There is no formal cybersecurity coordination in the organization to combat potential breaches.

Tier 2 - Risk Informed

Tier 2 organizations have started to formalize their cybersecurity efforts. You may have secured the seal of approval from management on processes and prioritization, but an organization-wide coordinated effort has yet to be launched. Your stakeholders may have a high-level awareness of potential threats, but they're unsure exactly how to respond to them and are only at the stage of informal sharing of information and coordinating efforts. Though adequate resources have been allocated to the efforts, your efforts haven't quite gotten off the ground yet.

Tier 3 - Repeatable

If your company falls into the Repeatable Tier, you have established formal policies that define risk management, and you have implemented practices to address these cybersecurity risks. Your processes are regularly reviewed and updated to ensure you are adequately prepared whenever a breach does occur. You have earned buy-in from your entire organization, and you have regular, formalized coordination on putting cybersecurity best practices into action.

Tier 4 - Adaptive

The organizations that have reached Tier 4 have mastered the adaptive approach to cybersecurity management. Their practices regularly adapt based on past experiences and future predictions. Cybersecurity best practices are ingrained in the organization's culture, and all stakeholders are actively working toward better security outcomes.

Which of these Tiers does your organization fall into, and based on these Tiers, what actions should you take to further improve on your data security practices? Evaluate the state of your cybersecurity measures carefully to determine which Tier your organization falls into and strategize with your stakeholders on how to ensure you can move up to the next Tier.

How Do You Use the NIST Cybersecurity Framework?

Now that you have a more comprehensive understanding of the NIST Cybersecurity Framework, you are ready to use it in your own business. There are three main ways that you can apply the framework to your business: building or supplementing your security practices, communicating expectations and establishing uniformity with your partner businesses, and identifying gaps in your current security processes that you need to be addressed.

First, consider how you can use the Framework in connection with your security processes. Whether your business is large or small, the NIST Cybersecurity Framework can be used to as a thorough set of recommendations for your data security practices. The Framework can act as a foundation for the security processes you are building for an entirely new business, or it can provide supplementary guidance on how to augment your existing security measures.

Next, the Framework provides the perfect set of expectations to be used in your partnership with other organizations. Regardless of how you plan to use the Framework, remember that it was designed to be flexible, meaning no two organization are likely to use it in the same way. However, it can create a universal set of guidelines for the partner organizations you work with each day to ensure your cybersecurity measures are in alignment. This helps you to mitigate the risk of a data breach through your interactions with other companies.

Finally, as you familiarize yourself with the NIST Cybersecurity Framework, use it to identify gaps in your company's data security activities and processes. Comparing the Framework to your current security policies can help your identify areas where updates are needed. For example, the Framework can help you consider information privacy and civil liberty implications as they pertain to a cybersecurity program.

Identifying gaps and updating your policies should not be a one-time occurrence, either, as NIST occasionally issues updates their policies. You should regularly revisit and reassess your security practices to determine if there are areas where updates are needed.

What Role Does Secure File Sharing Play in Using the NIST Cybersecurity Framework?

There are numerous ways that you could apply the NIST Framework to your organization. However, adopting a compliant secure file sharing solution makes the process of aligning with these security measures infinitely easier.

Instead of working to integrate multiple separate security practices, you could adopt a secure file sharing solution that has all the appropriate measures built-in. By simply adopting the solution and implementing it within your team, you would already be in alignment with the NIST Framework.

For example, the Detect Function recommends that you have detection processes in place to determine if a breach has occurred. A secure file sharing solution like FTP Today provides multiple firewalls with rapid intruder detection. Not only does this software detect the presence of an intruder, it automatically blacklists the intruder across all FTP Today's entire network of servers.

If you want to be in true alignment with the NIST Framework, your best option is to adopt a secure file sharing solution. During the search process, be sure to discuss your interest in the NIST Framework with the vendors you're considering and ask how their solution aligns with NIST's recommendations.

Ultimately, applying the NIST Framework to your organization holds a number of measurable cybersecurity benefits. Ensure you are among the numerous companies using the NIST Framework in the years to come. You're sure to see an increase in data security and a decrease in devastating cybersecurity attacks.

Find out how a secure file sharing solution can help you align with the NIST Cybersecurity Framework.

Schedule a live demo of FTP Today's GOVFTP solution.

Schedule My Demo →

FTP TODAY

About FTP

FTP Today specializes in Secure FTP file transfers utilizing a proprietary SaaS platform. Launched in 2001 after founder Martin Horan recognized the need for an FTP hosting specialty company, FTP Today became the first to build and directly market the technology of online managed file transfer via FTP and related protocols. We quickly made it to the top of our industry, and today we remain the company that all others follow. All common encrypted file transfer protocols are supported, which makes our service compatible with every legacy system and operating platform, from mobile to mainframe. With this compatibility comes automation -- something ignored by today's file sharing alternatives. FTP Today is proud to be the world's dominant secure FTP hosting specialist and the service that all our competitors try to copy. For more information, visit **www.ftptoday.com.**