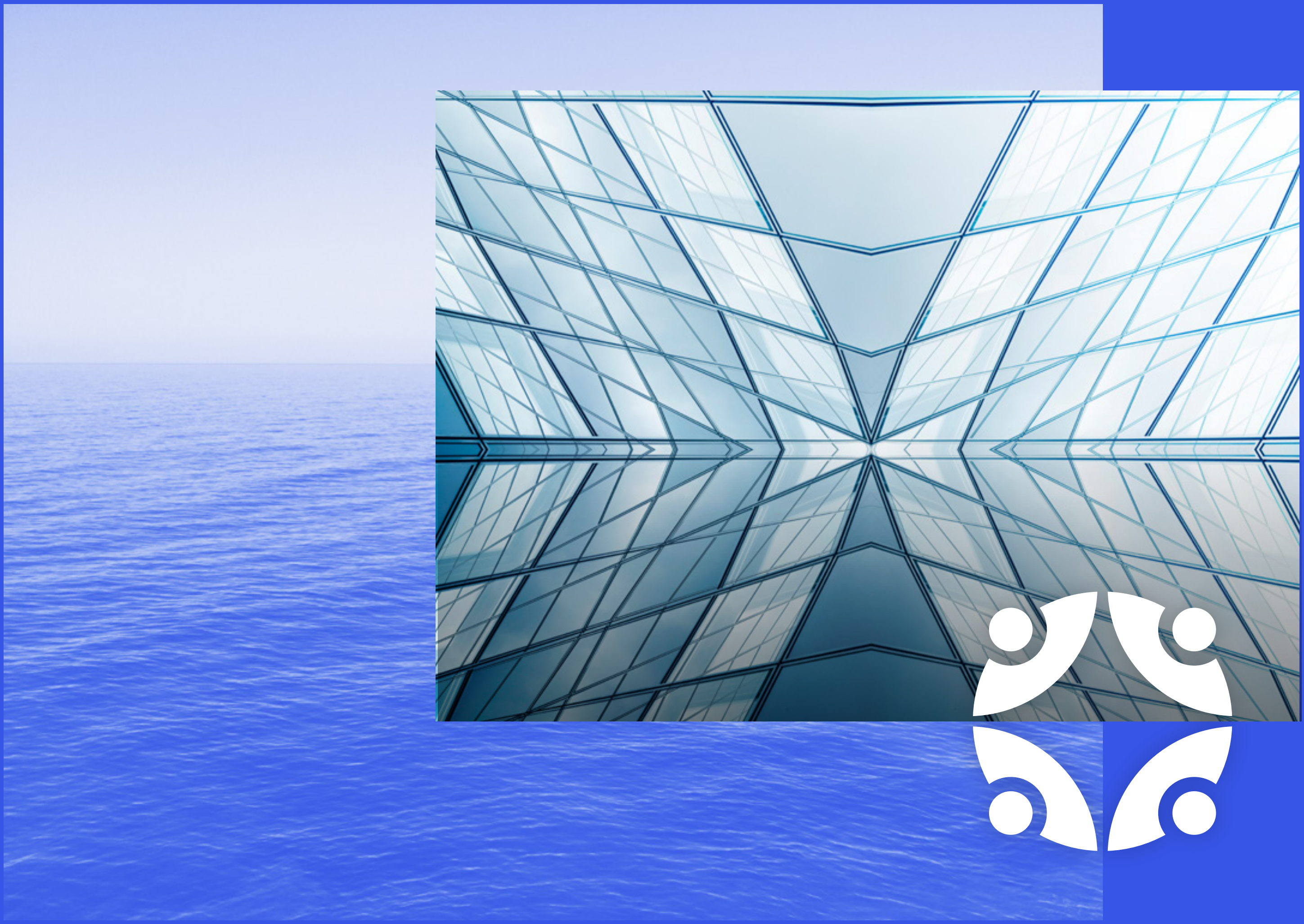
Clearwater

Whitepaper



How the NIST Cybersecurity Framework Helps Healthcare Organizations Establish and Mature Cybersecurity Programs

ClearwaterSecurity.com

Healthcare—Secure, Compliant, Resilient

Table of Contents

Introduction

Following the coronavirus outbreak of 2020, many organizations across a vast array of industries moved to fully or partially remote teams, increasing potential attack vectors, and healthcare centered right in attackers' sights.

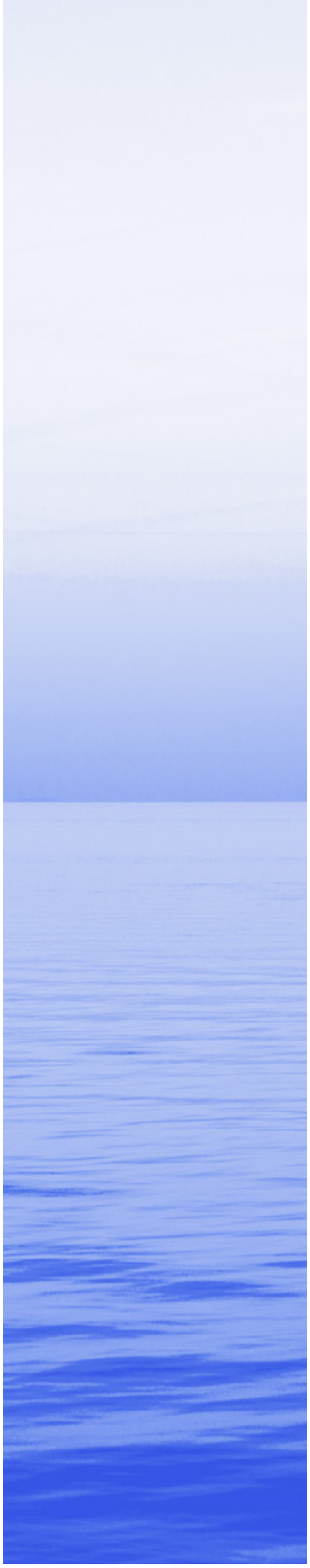
Since November 2020, the industry has experienced a 45% increase in cyberattacks, with phishing attacks, credential harvesting, and ransomware among the leading causes of security breaches.

Many healthcare cybersecurity, privacy, and compliance teams were already stretched prior to the pandemic, but changes with remote work environments upped the potential for attacks, meaning those teams could no longer just focus on internal protections for data and security, but now also remote networks where team members could potentially access sensitive or protected data from a variety of professional and personal devices.

These risks aren't just theoretical. In the first three months of 2021, the Office for Civil Rights (OCR) has already launched more than 100 investigations into data breaches that affected 500 or more individuals. Through this same time last year, in the early stages of the outbreak, OCR had almost 70 investigations underway.

These data breaches can have significant impacts on covered entities and they come with hefty costs. On average, a healthcare breach can cost more than $7 million per breach. But the effects are far-reaching. Covered entities that experience an attack may also have to deal with:

- Attack investigations (forensics)
- Rebuilding systems
- Restoring data
- Paying ransom
- Data breach notifications
- Potential civil penalties
- Potential OCR settlements
- Disruption of non-emergency clinical care
- Disruption of emergency services



- Serious patient injury or harm
- Diversion of patients
- Cancellation of elective surgeries

These risks, and the increasing number of attacks, are a call-to-action for all healthcare organizations to ensure they're making cybersecurity a priority, and that they're allocating appropriate resources and funding to their cyber risk management programs to ensure they can stay ahead of attackers and protect the sensitive data they're entrusted with.

Adopting a security framework

When it comes to establishing a cybersecurity program or improving existing security practices, many healthcare entities, especially small and mid-sized organizations, don't know where to begin. They're cautious to get started because they fear they won't have the funding, resources, or talent pool needed to tackle all of today's privacy and security challenges.

While security standards and regulations can be complex, starting your cybersecurity program doesn't have to be. With the right tools, you can adopt a phased approach to establishing and maturing your program with confidence you're investing on priorities that matter most to your organization.

So where do you begin?

While HIPAA is the key regulatory standard—and all covered entities and business associates must comply—you may find it helpful to adopt and implement a cybersecurity framework that is aligned with today's complex and evolving threat landscape.

The NIST Cybersecurity Framework, for example, is a free cybersecurity framework you can use to establish and mature your security program. It's not mandatory, so you don't have to attain a certification (and additional expenses). Rather, it's voluntary guidance based on existing industry standards and guidelines. You can use the framework as a living document to adjust and adapt as your organization evolves and your security program matures over time.

What is the NIST cybersecurity framework?

According to the National Institute of Standards and Technology (NIST), its Cybersecurity Framework helps organizations address threats while supporting business.

The framework is the result of collaboration between private sector industry professionals and government agencies. It was borne out of Executive Order 13636, which focused on improving critical infrastructure cybersecurity. Healthcare is one of the 16 critical infrastructure sectors.

The framework integrates industry best practices and standards into a common language to help organizations understand and communicate risks internally and externally throughout their supply chain.

The preliminary voluntary framework came out in 2013, with version 1.0 released the following year, defining its core and implementation tiers and establishing controls, security functions, categories, subcategories, and more.

- With the Cybersecurity Enhancement Act of 2014, Congress ratified these voluntary standards into NIST responsibilities. The framework is designed to help organizations:
- Identify risks, vulnerabilities and their potential impact
- Inform response
- Recover from incidents
- Evaluate root causes for weaknesses and vulnerabilities
- Take steps to improve controls to reduce risks

This framework, however, has not remained static and is evolving along with today's modern threat landscape. In 2018, for example, it was expanded to include self-assessments, supply chain risk management, identity and access management, and the vulnerability disclosure lifecycle.

And more changes are anticipated in the future, including:

- Cyberattack lifecycle: automated indicator sharing and data analytics
- Internet of things (IoT)
- Artificial intelligence (AI) and machine learning
- Measuring cybersecurity

- Referencing techniques
- Secure software development
- Governance and enterprise risk management

NIST framework overview

The NIST Cybersecurity Framework aligns to the cybersecurity program management lifecycle. It has five core functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

These five functions have an additional 23 related categories (think: control families) and another 108 subcategories (think: controls).

You can take a phased approach to implementing these core functions, categories, and subcategories, beginning at partial implementation, and then move upward in program maturity to risk-informed, repeatable, and adaptive stages.

On each side of the framework, you should also focus on governance and communication, which are important supporting elements for framework implementation and program management.

Selecting a framework

While the NIST Cybersecurity Framework is adaptable for organizations of all sizes across a range of industries, you may be curious if it's right for you. How do you know if this or another framework may better suit your needs?

Before you settle on a framework and get to work implementing it, consider conducting a business impact analysis (BIA).

A BIA will give you insight into your critical business functions and help you map those functions to your organization's missions and objectives. You'll also be able to:

- Identify which critical systems (think assets) support your most critical functions
- Understand your risk tolerances
- Identify regulatory and compliance requirements throughout your organization
- Identify existing threats and vulnerabilities
- Make a plan to address gaps and weaknesses
- Document those plans

Once you've determined those critical processes and assets—and have a better understanding of your strengths and weaknesses—you'll be better prepared to select the framework that best meets your organization's priorities.

8 steps to effective cybersecurity using the NIST framework

Once you've determined which cybersecurity framework is best for your organization, now it's time to set up your cybersecurity program. Or, if you already have one in place, you can use these recommendations to make improvements to your existing practices.

1. **Prioritize and scope**
    a. Identify business and mission objectives
    b. Determine the scope of systems supporting business units and processes
    c. Understand your risk tolerances
2. **Orient**
    a. Identify related systems and assets
    b. Identify regulatory requirements
    c. Identify current threats, vulnerabilities, known issues (from prior risk assessments, etc.)

Note: Some organizations struggle to get their arms around all of their assets, especially when they're often distributed across multiple departments or divisions within your organization. However, this is a critical step. If you can't identify all of your assets, you can't protect them. If they're not protected, you can't detect activity. If you can't see activity across all of your assets, you can't respond to issues or harden your *systems. Identification first is a core function because without it, you can't do the rest of these steps.*

3. **Create a current profile**
    a. Evaluate which framework categories and subcategories outcomes your organization currently achieves
    b. Establish a baseline for your program
4. **Conduct a risk assessment**
    a. Analyze your operational environment
    b. Determine likelihood and impact of a cybersecurity event
5. **Create a target profile**
    a. Develop criteria for target profile using framework categories and subcategories (think of this as where you want to be)
    b. Consider unique organizational risks and external stakeholders
    c. Document target profile
6. **Determine, analyze and prioritize gaps**
    a. Compare current profile to target profile and determine gaps
    b. Consider mission drivers, costs and benefits and risks
    c. Prioritize action plan
7. **Implement your action plan**
    a. Assign responsibilities
    b. Track and manage progress
8. **Repeat to continuously improve**

Getting executive buy-in and the role of governance for program success

Earlier, we mentioned how the NIST Cybersecurity Framework, which aligns to the cybersecurity lifecycle, is supported on either end by governance and communication. Both of these are supporting components of successful and mature cyber risk management programs. Without governance, you're just implementing controls. And while those controls may meet minimum HIPAA compliance standards, are you really building a program that keeps your sensitive data as safe as you should?

Traditional cybersecurity risk analysis generally focuses on technology solutions and detailed technical configurations. When new risks are discovered, even if they're critical or high severity, many organizations just don't have the funding, resources or staffing required for successful remediation, and oftentimes there can be a significant time delay between discovering the risk and getting all the tools a team needs to resolve it, sometimes spanning a year or longer until a new budget cycle.

What happens in the interim is repeated vulnerability assessments uncover new risks and the list grows longer, creating a snowball effect that overwhelms your teams who never work all the way through their list of remediation tasks and most struggle with the ability to prioritize which to work on first with their limited resources.

This is why governance is a crucial component of your framework-aligned program. It helps you facilitate involvement with your executives and key stakeholders and helps you develop effective communications that align your program goals with your organization's mission and objectives.

Here's a look at some key elements of successful and efficient governance you should consider when adopting the NIST Cybersecurity Framework:

- **Principles:** Your five core principles should relay your program intent to your board and define your organization's information security expectations. Using the NIST Cybersecurity Framework, one can simply adopt the Framework's 5 Core Functions as Principle Statements for your organization. Examples include: Identify, Protect, Detect, Respond, and Recover.
- **Policy statements:** Your leadership team should define and accept policy statements (for example, the framework's 23 categories) that are aligned to meet the intent of your cybersecurity principles. Examples include: Asset Management, Governance, Business Environment, Risk Assessment, Risk Management, Supply Chain Risk Management.

- **Directives:** Your directives should align to each subcategory level. These directives can further define expectations or your policy statements and should also align with your framework standards. Examples include: Physical Asset Inventory, Software Inventory, External Systems, Critical Suppliers, and Roles & Responsibilities.
- **Security standards:** Your security standards should be based on the framework's pre-defined standards and controls referenced from CIS, ISO 27002, and ISO 27005. You can customize these controls based on your organization's needs. Examples include: Physical Device Inventory Standards, Software Inventory Standards, Server Patch Management Standards, Workstation Patch Management Standards, and Server Hardening Standards.
- **Procedures and guidelines:** Your procedures should outline your security-related processes, activities, and methods to implement and maintain requirements your security standards define. For guidelines, develop these as pragmatic advice about how to fulfill your security standard requirements. Most teams consider guidance and advice as discretionary, but it should be clear to your teams that the underlying requirements are mandatory.

When you engage with your executives with governance at the forefront, you can better demonstrate to your stakeholders your current profile, your target profile, and your future vision for your program. You can also use your action plan to illustrate where you have gaps and weaknesses and what you need in terms of resources and financial support to close these gaps.

Critical foundational components

Critical cybersecurity program governance components for successful adoption of a framework such as the NIST Framework include: Cybersecurity Program Charter, Cybersecurity Oversight Committee, Program Measurement and Monitoring expectations, Multi-year Cybersecurity Strategic Work Plans, and Annual Tactical Work Plans (critical in budgeting and effort prioritization).

Evaluating your current profile for future success

If you're not sure how to evaluate your current profile against the NIST Cybersecurity Framework or set the baseline for your security program, Clearwater can help. Clearwater's Performance Measurement Model identifies individual cybersecurity controls status by isolating and evaluating control-building blocks and their level of adoption, including definition, implementation, evolvement, and validation. It then issues maturity ratings for roughly 300 Framework aligned controls, including:

- Control expectations are not defined or implemented
- Control expectations are defined (policy, procedure, standard, guideline)
- Control expectations are implemented
- Control expectations are repeated or reported (managed)
- Control expectations regularly reviewed and updated (improved)
- Control expectations are internally audited (validated)

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact