vertikal 6
TECHNOLOGY. ELEVATED.

THE NIST GUIDE FOR SMALL BUSINESSES

Structured Cybersecurity for Your Organization

Safeguarding sensitive data, protecting intellectual property, and ensuring the steady operation of critical IT infrastructure fall on the shoulders of businesses of all sizes.

The specter of cyberattacks is looming larger with each passing day, casting a longer shadow over small and medium-sized businesses (SMBs). These SMBs often find themselves in the crosshairs, generally less armored than their larger counterparts against the sophisticated arsenals of cybercriminals.

There is help by way of an invaluable risk management tool: The National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

Created to shield the Department of Defense and US critical infrastructure, the scope of NIST Cybersecurity Framework extends far beyond, embracing any organization that juggles sensitive information and relies on IT infrastructure for its day-to-day operations.

This guide breaks down the essentials of NIST Cybersecurity Framework to help you bolster your existing cybersecurity measures or get started on implementing core standards within your organization.

What Is the NIST Cybersecurity Framework?

Created by the National Institute of Standards and Technology, the Cybersecurity Framework was first published in 2014, rapidly ascending to the pedestal of cybersecurity gold standard across a spectrum of industry sectors.

The vision of NIST was clear: to create a shared set of standards, objectives, and language to empower organizations to not only thwart cyberattacks but also bounce back with ease.

NIST Cybersecurity Framework is written simply, extending a hand towards those with limited IT security expertise, and offering a pathway to integrate its standards into their cybersecurity blueprint.

The Components of the NIST Cybersecurity Framework

While the subject matter is detailed, at its heart NIST Cybersecurity Framework consists of three main components:

Framework Core

Defined as "a set of desired cybersecurity activities and outcomes using common language that is easy to understand," it aims to guide organizations in managing and diminishing cybersecurity risks by integrating with existing protocols.

Framework Implementation Tiers

These tiers gauge an organization's stance towards cybersecurity risk management, spotlighting the extent to which the NIST Cybersecurity Framework has been embraced.

- **Tier 1 –** Partial
- **Tier 2 –** Risk-informed
- **Tier 3 –** Repeatable
- **Tier 4 –** Adaptive

Not every organization may find it viable to adopt the NIST Cybersecurity Framework in its entirety across all IT operations. These tiers afford the latitude to pinpoint the optimal level of rigor for distinct cybersecurity processes.

Framework Profiles

Envisioned as "an organization's unique alignment of their organization's requirements and objectives, risk appetites, and resources against the desired outcomes of the Framework Core," its primary intent is to spotlight and prioritize actions that could elevate an organization's cybersecurity stature.

These three components are organized into five quintessential functions of cybersecurity:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

When applied collectively, these components and functions ensure a holistic and proactive approach to cybersecurity. Let's take a deeper look at the five functions of cybersecurity.

Identify

- Identify Critical Processes & Assets
- Identify Threats, Vulnerabilities & Risks
- Document Information Flows
- Maintain Inventory of Software & Hardware
- Establish Cybersecurity Policies With Roles & Responsibilities

Protect

- Manage Access
- Protect Sensitive Data
- Protect Devices
- Conduct Regular Backups
- Train Users

Detect

- Test & Update Detection Processes
- Maintain & Monitor Logs
- Understand Your Organization's Expected Data Flows
- Understand Cybersecurity Event Impacts

Respond

- Test Response Plans
- Update Response Plans
- Internal & External Stakeholder Coordination

Recover

- Internal & External Stakeholder Coordination
- Update Recovery Plans
- Manage Organizational Reputation

Five Functions of the NIST Cybersecurity Framework

Ensuring a digital safety strategy is crucial for any organization. The NIST Cybersecurity Framework streamlines this process by categorizing cybersecurity measures into five essential functions.

1. IDENTIFY

Understanding the landscape is the first step towards fortifying your organization against cyber threats.

Identify Critical Processes & Assets
Pinpoint the gears that keep your organization running smoothly. What are the assets that, if compromised, could stagger your operations?

Identify Threats, Vulnerabilities & Risks
Establish a system to monitor and assess potential threats and vulnerabilities continuously, keeping the risk register updated.

Document Information Flows
Map out your data, understanding where it resides, how it moves, and who has access to it.

Maintain Inventory of Software & Hardware
Know your digital terrain by maintaining an updated inventory of all software and hardware assets.

Establish Cybersecurity Policies With Roles & Responsibilities
Create comprehensive cybersecurity policies that outline roles and protocols, ensuring everyone is prepared.

2. PROTECT

Building a fortress around your data is imperative to thwart potential intrusions.

Manage Access
Ensure that access to sensitive assets is on a need-to-know basis, with authenticated and unique user credentials.

Protect Sensitive Data
Encrypt sensitive data whether at rest or in transit and be sure of its secure disposal when no longer needed.

Protect Devices
Safeguard your devices with host-based firewalls and endpoint security solutions, keeping them tuned for optimum security.

Conduct Regular Backups
Regular backups are your safety net against data loss. Ensure a set of backups is kept offline to guard against ransomware attacks.

Train Users
Equip your team with the knowledge and best practices to recognize and prevent potential cyber threats.

3. DETECT

Early detection of anomalies can significantly curtail the damage potential of cybersecurity incidents.

Test & Update Detection Processes
Regularly test and fine tune your detection systems to stay ahead of potential intruders.

Maintain & Monitor Logs
Detailed logs can be a treasure trove of information to spot irregular activities early on.

Understand Your Organization's Expected Data Flows
Knowing the usual data traffic patterns helps in identifying anomalies quickly.

Understand Cybersecurity Event Impacts
Should an incident occur, assessing its impact properly can expedite the mitigation process.

4. RESPOND

A well-orchestrated response can mitigate damage and restore normalcy.

Test Response Plans
Regular drills to test your response plans assure that your team is ready to spring into action when needed.

Update Response Plans
Post-drill evaluations often unveil areas for improvement. Keep refining your response plans for better preparedness.

Internal & External Stakeholder Coordination
Coordinated response, involving all stakeholders, paves the way for an effective mitigation strategy.

5. RECOVER

Resilience in the face of adversity is the hallmark of a mature cybersecurity posture.

Internal & External Stakeholder Coordination
Again, transparent communication with stakeholders is crucial for systematic recovery.

Update Recovery Plans
Lessons learned from incidents should be integrated into updated recovery plans, enforcing a culture of continuous improvement.

Manage Organizational Reputation
Strategize on how to communicate incidents externally to uphold your organization's reputation so stakeholders remain confident in your cybersecurity measures.

Advance Your Cybersecurity

Cyber threats evolve at a pace that can be overwhelming for SMBs. The NIST Cybersecurity Framework lays down a structured approach to understanding, managing, and mitigating security risks. However, its implementation may present a challenge, especially for SMBs with limited IT resources or those without a dedicated IT division.

That's where Vertikal6 bridges the gap. We're here to assist you in evaluating your current cybersecurity posture and guide you towards NIST Cybersecurity Framework compliance in alignment with your unique organizational concerns.

Our suite of advanced security technologies and vigilant monitoring mechanisms surpasses the basic NIST Cybersecurity Framework guidelines, so you can be confident your organization has the most robust cybersecurity measures in place.

Connect with our expert advisors for a free, no-obligation strategy consultation, and let's explore how we can deliver a secure, resilient, and compliant operational environment for your organization.