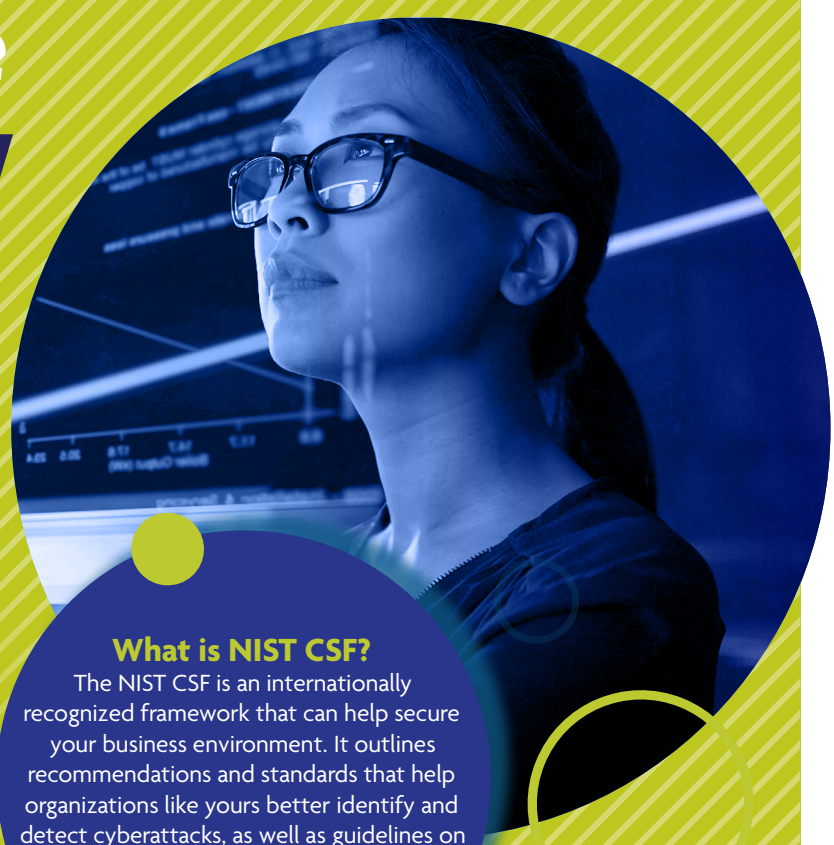
Understanding the NIST Cybersecurity Framework for Your Business

A small business like yours is a much easier and lower-risk environment for hackers to test their skills and launch attacks. A clear understanding of your organization's cybersecurity posture is more important than ever as cyberthreats and hackers continue to advance in numbers and sophistication. Solid cybersecurity isn't a pipe dream as many business owners believe. The NIST Cybersecurity Framework (CSF) enables you to strengthen your organization's cybersecurity posture; however, it requires knowledge of what it is and how it works to be successful.



What is NIST CSF?

The NIST CSF is an internationally recognized framework that can help secure your business environment. It outlines recommendations and standards that help organizations like yours better identify and detect cyberattacks, as well as guidelines on how to respond, prevent and recover in the event of an incident.

5 Key Elements of the NIST CSF

IDENTIFY

A comprehensive understanding of your IT environment is essential to managing your cybersecurity risk. Ensure you have complete visibility over your digital and physical assets, so you can clearly define each asset's role and responsibility. This will enable you to identify risks and create policies and procedures for dealing with them.

PROTECT

You should focus on limiting the potential consequences of a cybersecurity compromise. Your IT service provider should maintain track of both digital and physical resources, create awareness and training, preserve data, and monitor network configuration baselines and operations. Using this approach will accelerate the rectification of compromised system components. You should also employ preventive technologies to increase cyber resilience.

DETECT

To identify cybersecurity events before they cause real damage, you need the right metrics. System monitoring is required to identify anomalous behavior and threats to your daily operations. You need 360-degree visibility into your corporate networks to detect a cyberattack in advance and respond properly. Constant surveillance is the best way to spot and prevent intrusions on your IT networks.

RESPOND

When a cyber incident impacts your company, you must create a response plan, identify the appropriate lines of communication, collect and examine case data, take all required steps to end the problem and apply any lessons learned to your new response.

RECOVER

The recovery phase of your incident response plan focuses on restoring the affected systems after an attack or incident. You must ensure your affected systems are tested, monitored and verified during this phase to prevent a similar catastrophe in the future.

4 Common Myths About the NIST CSF framework

MYTH 1
NIST CSF only applies to U.S.-based organizations.

TRUTH: Although the NIST CSF standards were developed by a U.S. entity, this does not imply they only apply to U.S.-based businesses. This methodology can help organizations worldwide better understand, manage and lower potential cybersecurity threats.

MYTH 2
NIST CSF is a product I can buy.

TRUTH: NIST CSF is not a software but a framework for implementing a best-in-class cybersecurity program. You can partner with IT service providers to build comprehensive cybersecurity programs that are vendor agnostic.

MYTH 3
Everyone has to implement all of NIST CSF.

TRUTH: The NIST CSF can be implemented to improve cybersecurity and compliance, but it might be overly comprehensive in some cases. Applying fundamental concepts while customizing for your unique use case is possible with the aid of an IT service provider.

MYTH 4
I can skip certain pieces of NIST CSF.

TRUTH: Although you can skip certain pieces, it's crucial to document why. Your IT service provider can help you maintain compliance with the standards you've decided to uphold while helping you continue to accomplish your primary cybersecurity **goals**.

How an IT Service Provider can help

Adhering to the NIST framework is a good security hygiene practice for your organization. However, it is tough to implement any changes successfully — or even know what changes to make and how without an expert. An IT service provider like us has the in-depth knowledge to utilize the CSF effectively and develop a strong cybersecurity posture for your company that can safeguard your business from ransomware attacks, phishing scams, data loss and technical difficulties.

Ensure your cybersecurity is top-notch. Contact us today to make your business cyber-secure by utilizing the NIST CSF.