Cybersecurity, the ability to protect or defend the use of **cyberspace** from **cyberattacks**. is increasingly critical to both the general public and **small businesses**. One organization leading the way is the National Institute of Standards and Technology (NIST), who recently marked the five year anniversary of their comprehensive *NIST Cybersecurity Framework*.

Established in 1901, the National Institute of Standards and Technology (NIST) is a nonregulatory agency of the U.S. Department of Commerce. The mission of NIST is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." Headquartered in Gaithersburg, MD with a satellite location in Boulder, CO, NIST employs about 3,400 scientists, engineers, technicians, and support and administrative personnel. NIST conducts its work through the following programs: the NIST Laboratories, the Hollings Manufacturing Extension Partnerships, and the Baldrige Performance Excellence Program.

Leading the Way for Five Years

Released in 2014, this February marked the fifth anniversary of the *NIST Cybersecurity Framework*. The Framework for Improving Critical Infrastructure Cybersecurity is an approach consisting of standards, guidelines, and best practices to manage cybersecurity-related risks. The efforts to develop the framework were made possible through a year-long collaboration of hundreds of organizations from industry, academia, and government agencies. Since its release, the framework has been downloaded more than half a million times with the first update, Version 1.1 released in April 2018, downloaded more than 267,000 times. The framework has been translated into multiples languages and is a reference for frameworks in other countries.

The Framework

According to NIST, Initial development of the framework was to safeguard our nation's most critical infrastructure, such as transportation and the electric power grid. Today, the framework extends beyond infrastructure and applies to a broader aspect of society. Although voluntary for the private sector, compliance with the framework is mandatory for all U.S. federal agencies per a 2017 Presidential executive order.

Cybersecurity and Small Business

Utilizing third-party vendors for back-office systems to front-line payment processing systems exposes small businesses to numerous cybersecurity vulnerabilities. The various

risks inherent in the use of these operationally necessary systems can be costly. A 2017 report on the state of cybersecurity among small businesses by the Better Business Bureau states that the overall annual loss for small businesses is $79,841.

Resources

For more resources and information, visit our Cybersecurity page.

Interested in starting your own business or looking to grow your existing business? Find Your Local Small Business Development Center for no-cost business advice and free or low-cost trainings.

If you have a small business resource or SBDC story you think would make a great feature, please Contact Us.