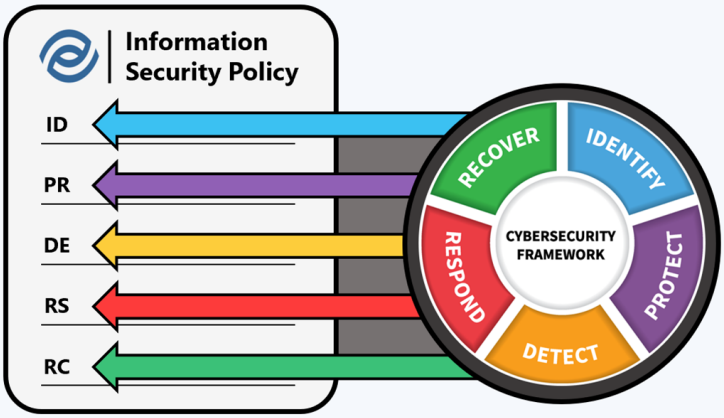
OPTIC CYBER SOLUTIONS

Cybersecurity Framework Success Story

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.



"Leveraging the Cybersecurity Framework has helped us to streamline our capabilities & ensure we have consistent communication with our team and our clients."

-Kelly Hood, EVP & Cybersecurity Engineer

Organizational Profile

Optic Cyber Solutions (Optic) is a veteran owned small business located in Maryland. Optic works with many industries (e.g., education, transportation, utilities) in support of securing U.S. critical infrastructure.

Optic provides cybersecurity assessment and consulting support to organizations to help build cyber resilience into their businesses. This support includes Optic's access to clients' sensitive data, therefore requiring the need for Optic to have a robust cybersecurity program to ensure the protection of the entrusted client data.

Situation

As a small business in the technology sector, it was important for Optic to choose a widely recognized and comprehensive cybersecurity framework that did not force rigid controls upon the organization. Additionally, Optic found the need to employ a framework that established a common language across sectors and amongst a variety of partners and clients.

As a team of cyber professionals, Optic understood the importance of having capabilities in place to protect against cyber threats which aided in the roll-out of internal cybersecurity initiatives.

Prior to implementation of the Cybersecurity Framework, there was an expectation that everyone understood what needed to be done from a cybersecurity perspective. Leveraging the Cybersecurity Framework enabled Optic to clearly communicate expectations internally to cybersecurity practitioners as well as externally to partners in industry to ensure that everyone is working towards the same goals.

Process

Optic primarily leveraged the Cybersecurity Framework's Core and Profiles to facilitate collaboration across its team. Using the Cybersecurity Framework, Optic was able to evaluate current cybersecurity capabilities and define its cybersecurity program.

Based on the team's knowledge of their current cybersecurity capabilities, Optic began conversations to better understand areas of potential weakness for each Subcategory within the Core.

Risk discussions allowed Optic to gain a clearer understanding of potential vulnerabilities and threats. This led to the documentation of a Risk Register helping to inform prioritization of cybersecurity improvements.

These risk-informed decisions guided the development of a Target State Profile, clarifying cybersecurity expectations across the organization.

- The Target State Profile defined strategic goals for each Subcategory in the Framework broken down by desired artifacts and activities.

Process (cont.)

Using the knowledge about current capabilities and the desired cybersecurity program targets, Optic formalized an Information Security Policy structured to reflect the Cybersecurity Framework.

- The Information Security Policy incorporates the Functions and Categories of the Cybersecurity Framework providing a foundation for defining the organizational directives essential for protecting Optic's business interests.

Leveraging the tools and processes created during the implementation of the Cybersecurity Framework, Optic then began a cycle of continuous improvements toward fulfilling the program goals defined in the Target State Profile.

- With the support of the entire team, Optic makes regular updates to the Information Security Policy and practices used for implementing them.
- Additionally, regular team meetings are held to facilitate opportunities for all employees to ask questions and to encourage active participation in the betterment of Optic's cybersecurity capabilities.

Results & Impact

The Cybersecurity Framework has enabled Optic to foster a culture of cybersecurity and empower conversations surrounding cyber risk.

Results & Impact (cont.)

- Creating a streamlined approach has enabled the team to more clearly define target capabilities and work more efficiently towards those goals.
- Using the Framework allowed Optic to gain insight into cybersecurity capabilities across all five Functions and ensure the overall resilience of their security processes.

The guidance provided by the Cybersecurity Framework through the Core and Informative References has enabled Optic to verify that comprehensive protections are implemented, and to prioritize improvement activities to fit security and operational needs.

The implementation process enabled Optic to more effectively manage and communicate expectations across the team to encourage risk-informed decision making.

- Additionally, Optic has found the Cybersecurity Framework to be an effective tool when collaborating with clients to enable more effective conversations between senior executives and cybersecurity practitioners.

Optic will continue to focus efforts on improving its cybersecurity posture as well as aiding other organizations in strengthening their capabilities through the use of the Cybersecurity Framework.

Contact Information & Resources

Kelly Hood, EVP & Cybersecurity Engineer
Info@OpticCyber.com
www.OpticCyber.com