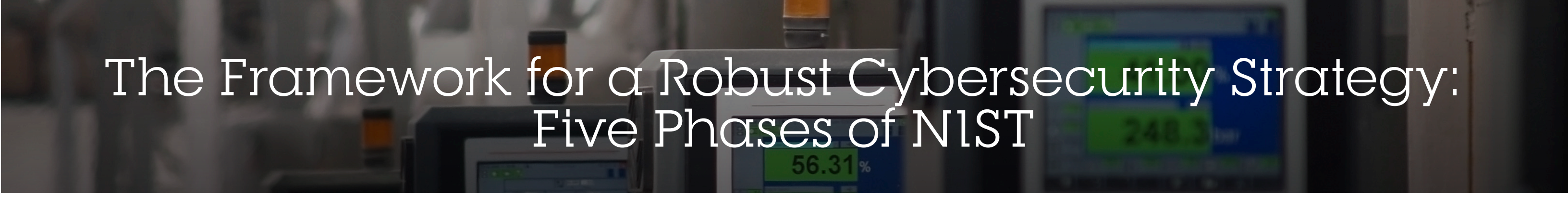
The Framework for Robust Cybersecurity Strategy

hargrove

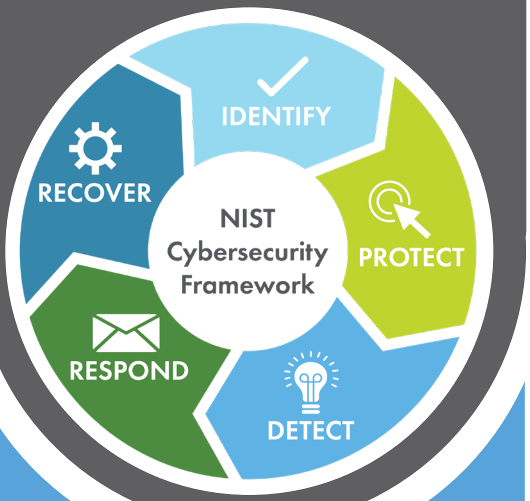
Operating within the National Institute of Standards and Technology (NIST) Cybersecurity Framework, we perform work that covers the five core functions of cybersecurity. From identifying the risk to implementing the protection, Hargrove works to ensure that our client sites are safe and secure throughout the information lifecycle.



The Framework for a Robust Cybersecurity Strategy: Five Phases of NIST

IT/OT & Cybersecurity Capabilities:

- Cybersecurity Perimeter Defense & Monitoring
- VMware & Hyper-V Virtualization Technologies
- Active Directory Domain Integration
- Secure Remote Access
- Server & PC Support
- Process Control Networking
- Industrial Wireless
- Ethernet Protocols
- OSI PI Historian Server
- SAP/Plant Information Integration
- Custom Plant Application Development & Support
- Industrial Control Systems (ICS)



Let's keep you secure. Contact us today.

1. Identify

In order to fight your enemy, you must know your enemy, and we consider identification to be the most important phase of implementing a robust cybersecurity strategy. We begin the Identify phase by defining your cybersecurity requirements, assessing the potential risks, and categorizing your assets in order to develop a holistic view of your systems and the cybersecurity environment. By initiating projects with the Identify phase, we ensure that we have a comprehensive understanding of the actions required to properly implement the recommended security controls that will help protect your people, data, and capabilities.

In this phase, the Hargrove Team:

- Identifies and documents the system assets
- Assesses the potential cybersecurity risks
- Works with your team to define your cybersecurity requirements

2. Protect

The Protect phase involves the technical configuration and security controls required to develop and implement appropriate safeguards. The Hargrove team utilizes our combined cybersecurity and engineering experience to design, check, and test the security controls most appropriate to your environment. These actions typically include activities such as network segmentation, user access controls, multifactor authentication, and physical safeguards.

In this phase, the Hargrove Team:

- Implements appropriate user access controls such as password requirements and least privilege permissions
- Designs secure system network architectures
- Implements physical safeguards such as USB barriers and cabinet locks

3. Detect

The importance of the Detect phase is critical to ensure your ongoing operations and the success of the security controls implemented in the Protect phase. If the Protect phase is about building your walls, the Detect phase involves putting guards on them. This includes the development and implementation of active protection systems such as Intrusion Detection Systems and Security Information Event Managers to identify the occurrence of a cybersecurity event. Actively monitoring the environment and looking for intrusions for anomalies alerts appropriate personnel for your best chance of responding before the breach can affect you.

For this phase, the Hargrove Team:

- Creates alarm protocols
- Implements Intrusion Detection Systems
- Trains operators to identify potential threats

4. Respond

Respond involves developing and implementing a plan for the activities that need to take place during a detected cybersecurity event. In the same way that we plan for emergencies and run fire drills, we need to develop and test our cybersecurity response strategy as well. This phase also addresses the communication and education requirements for embracing your new cybersecurity plan. Many operators respond with fear, thinking that the new system indicates a lack of trust. We communicate throughout the planning and implementation to explain the risks and how the new system addresses those risks so that the new system is welcomed by all stakeholders.

In this phase, the Hargrove Team:

- Defines and documents disaster recovery plans
- Works alongside your team to develop a clear communication plan so that there is no confusion when an event happens
- Works with operators or the system end users to help them understand the need for the new protocols

5. Recovery

After all of the Identification, Protection, Detection, and Response activities, there is sometimes still the need to recover your systems. From standard IT events such as loss of data or system corruption to partial or even full cybersecurity events, Recovery ensures that your plans are fully and properly implemented to get your systems back online as fast as possible and with full data validation.

For this phase, the Hargrove Team:

- Works with your team to develop protocols and choose appropriate systems for recovery
- Assists your team with implementing and completing planned recovery activities
- Facilities hardware procurement and configuration to replace impacted systems