MEP National Network™

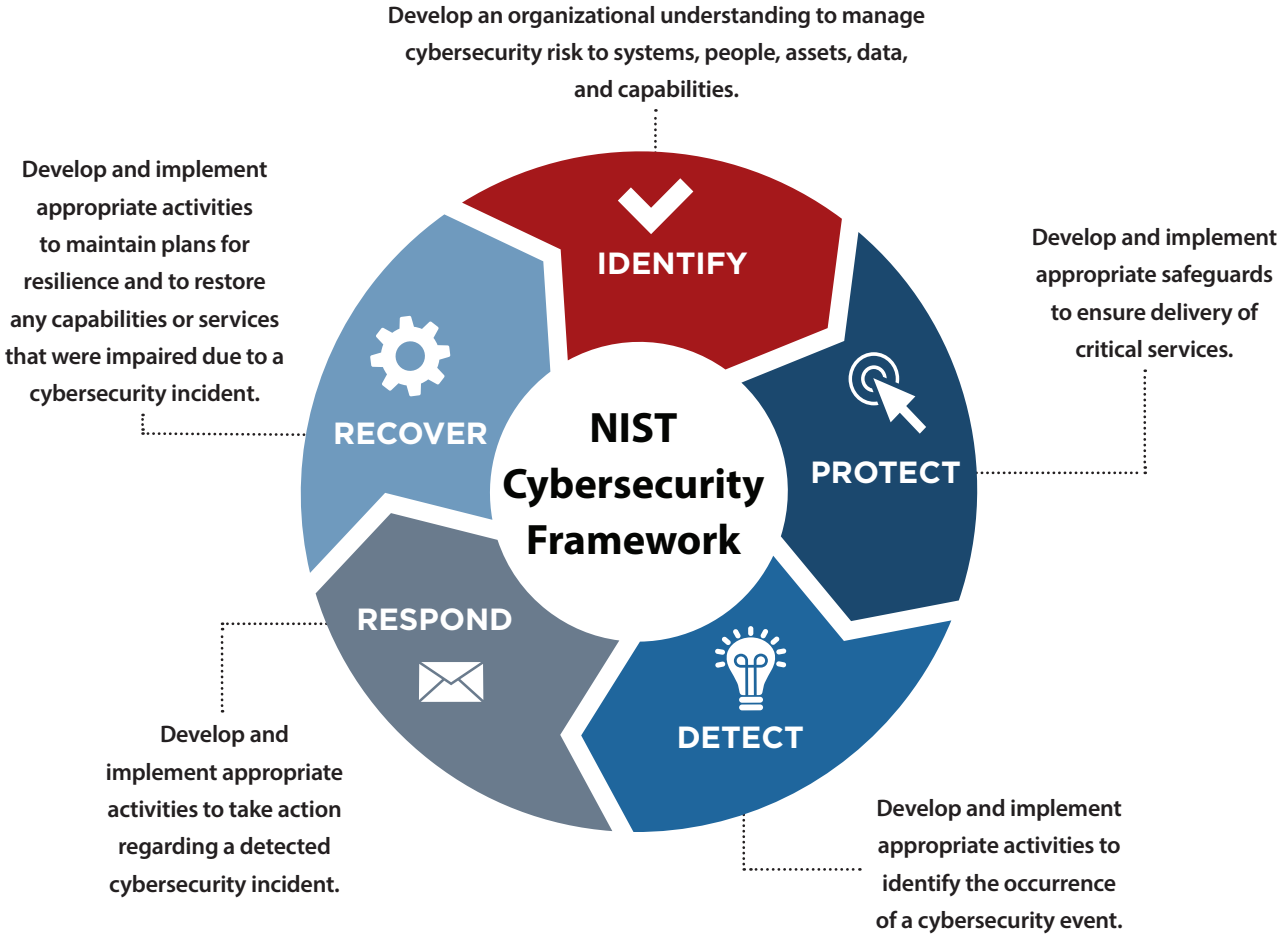
CYBERSECURITY

According to the US Department of Homeland Security, the manufacturing industry is the second most targeted industry when you look at the number of reported cyber attacks. Why? Cyber criminals view small and medium-sized manufacturers as prime targets precisely because many of these companies do not have adequate preventative measures in place.

With more than 289,000 small manufacturers in the United States, small manufacturers are a vital part of our nation's economic and cyber infrastructure. For most small manufacturers, the security of information, systems, and networks is not the highest priority, but a cybersecurity incident can be detrimental to the business, customers, or suppliers. It's important that manufacturers understand and manage the risk and establish a cybersecurity protocol to protect critical assets.

Five Steps to Reduce Cyber Risks

This resource is for small manufacturers to quickly and cost effectively address cybersecurity threats. These simple, low cost steps are based on the official NIST guidance from the Cybersecurity Framework and have been tailored to meet the needs of small companies so they can identify, assess and manage cybersecurity risks.



NIST Cybersecurity Framework

1. Identify

- Identify and control who has access to business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for cybersecurity

2. Protect

- Train employees and limit employee access to data
- Install surge protectors and uninterruptible power supplies
- Patch operating systems and applications routinely
- Install and activate firewalls on all business networks
- Secure wireless access points and networks
- Set up web and email filters
- Use encryption for sensitive information
- Dispose of old computers and media safely

3. Detect

- Install and update anti-virus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs
- Note unusual password activity

4. Respond

- Develop and maintain a plan for disasters and cyber incidents
- Notify your customers and the authorities

5. Recover

- Make full backups of important business data and information
- Schedule incremental backups
- Improve processes, procedures, and technologies

NIST National Institute of Standards and Technology
U.S. Department of Commerce

WWW.NIST.GOV/MEP/MEP-NATIONAL-NETWORK
1-800-MEP-4MFG • MFG@NIST.GOV