Cybersecurity Framework
Steps for Manufacturers

Why Cybersecurity Matters
Small manufacturers are a vital part of our nation’s economic and cyber infrastructure. There are over 289,000¹ small manufacturers in the U.S. In 2015, the average cost of a data breach for small companies was $38,000². It has been estimated that more than half of the companies go out of business within six months of a cyber attack³.

For most small manufacturers, the security of your information, systems, and networks is not the highest priority given everything else you’re faced with. But an information security or cybersecurity incident can be detrimental to the business, your customers, partners, or suppliers. It’s important that manufacturers understand and manage the risk and establish a cybersecurity protocol to protect your most 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.

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

2. **PROTECT**
   - Limit employee access to data and information
   - Install Surge Protectors and Uninterruptible Power Supplies (UPS)
   - Patch your operating systems and applications routinely
   - Install and activate software and hardware firewalls on all your business networks
   - Secure your wireless access point and networks
   - Set up web and email filters
   - Use encryption for sensitive business information
   - Dispose of old computers and media safely
   - Train your employees

3. **DETECT**
   - Install and update anti-virus, anti-spyware, and other anti-malware programs
   - Maintain and monitor logs

4. **RESPOND**
   - Develop a plan for disasters and information security incidents

5. **RECOVER**
   - Make full backups of important business data and information
   - Continue to schedule incremental backups
   - Consider cyber insurance
   - Make improvements to processes/procedures/technologies

For assistance, please contact your local MEP Center at 800-MEP-4MFG.

¹ 2014 County Business Patterns, United States Census Bureau
² 2015 Global IT Security Risks Survey, Kaspersky Lab
³ Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks, United States House of Representatives Committee on Small Business Cong. (April 22, 2015) (testimony of Dr. Jane LeClair)