MxD: Cybersecurity in Manufacturing

August 5, 2020

MxD Cyber

National Center for Cybersecurity in Manufacturing

"Securing America's Supply Chains"

TRAINING & AWARENESS

CYBERSECURITY TOOLS & SERVICES

CYBERSECURITY WORKFORCE PROGRAMS

COMPLIANCE

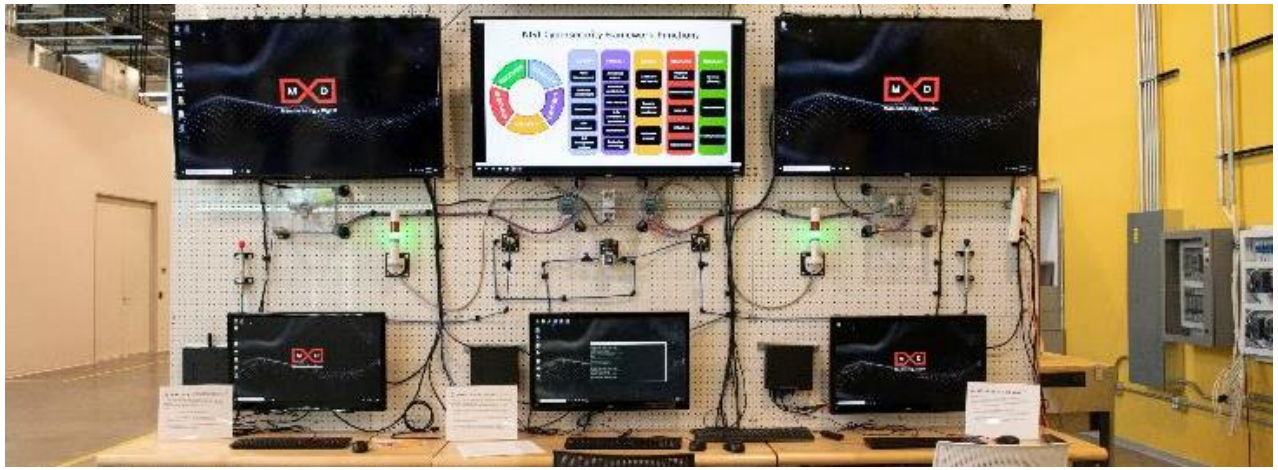
https://twitter.com/axios/status/1265755378773622785

01 Identify / Protect

Inventory of assets

Sufficient detail to inform protection

Defense in-depth



02 DETECT

Baselining

Anomaly

Notification

Analysis

Improvements

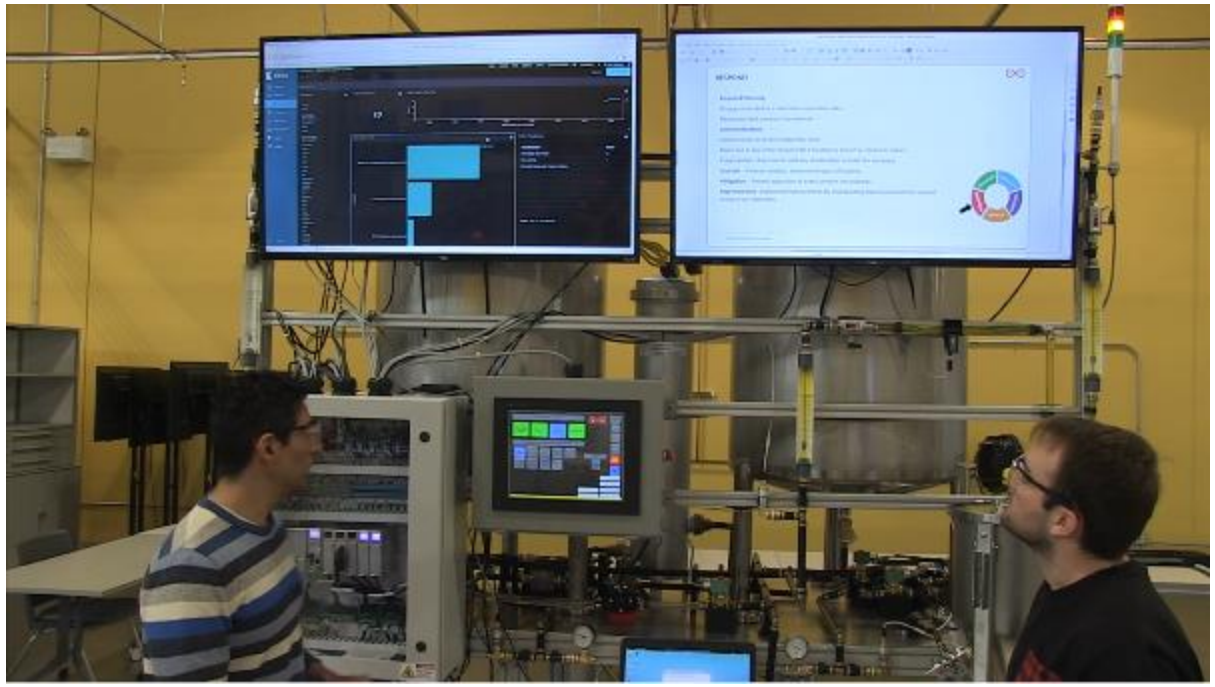
03 RESPOND

Containment

Communications

Analysis

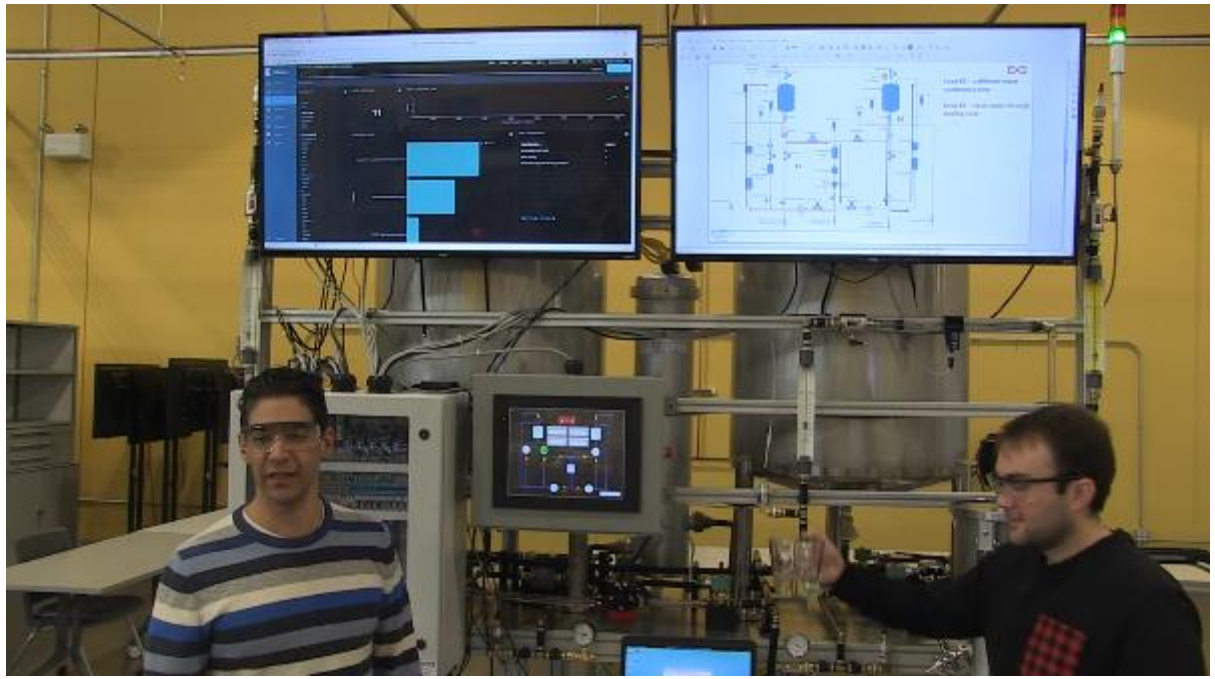
Improvements



04 RECOVER

Resiliency by Design

Robust Plan &Testing Exercises



19-12-02

ENABLING CYBERSECURITY FOR THE DIGITAL MFG. SUPPLY CHAIN

Benchmarking and evaluating cybersecurity tools for OT and IT asset inventory and network vulnerability assessments that are accessible to small and medium manufacturers.

Project Team: TBA

Estimated Duration: 9 months

Budget: $0.2M MxD Funding

Current Status: Pre-Award Negotiation

"As the person responsible for implementing our cybersecurity program at a small manufacturer, I want easy-to-use tools that can be easily understood without taking too much time away from my day job"

INDUSTRY CHALLENGE

- There is a lack of tools and expertise needed to identify and mitigate cyberattacks, especially for small and medium manufacturers in the supply chain. Moreover, traditional vulnerability assessment tools have targeted the discovery, validation, and testing of vulnerabilities in information technology systems. Solutions to be tested therefore must have capabilities that allow for testing of operations technology and information technology (OT/IT) components of manufacturing entities

IMPACT

- Report of benchmarking of existing cybersecurity tools: Documented set of criteria that is vital to an effective SMM cyber solution and benchmark tools on the listed functional/technical evaluation factors..
- Report from pilot implementation detailing analysis to validate the effectiveness of the benchmarking, identify solution gaps, and provide guidance for implementation that will help maximize ROI for SMMs.

PROJECT SOLUTION & OUTCOME

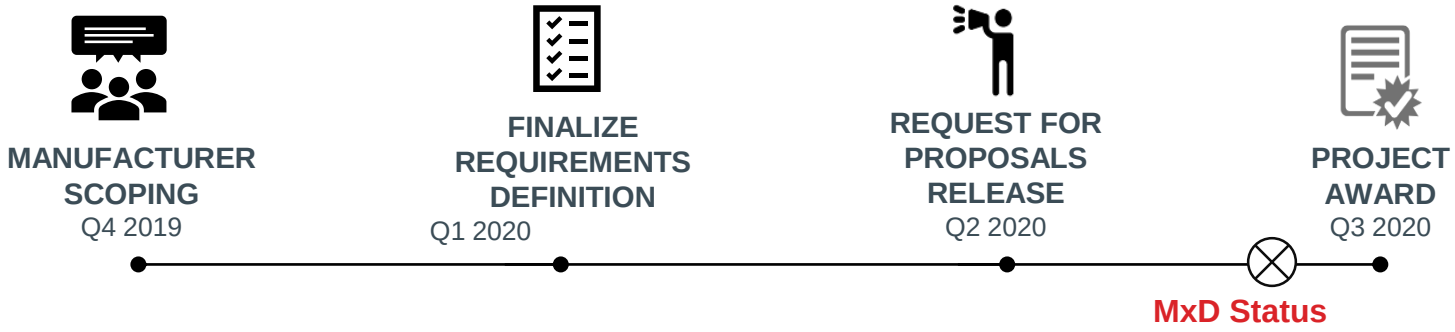
- Development and Identification of Cybersecurity Profile for Manufacturers: Develop or leverage existing literature for self-assessment profiles that helps manufacturers understand their current cybersecurity readiness/status and their unique needs relating to cybersecurity toolsets.
- Define/document criteria for benchmarking of existing Cybersecurity solutions.
- Report on performance of benchmarked tools based on established criteria: Conduct a pilot implementation and test of the top cybersecurity tools for vulnerability management and non-intrusive penetration testing from the benchmark assessment that matches the SMM's cyber profile.

20-01: CMMC READINESS ASSESSMENT

Problem Statement: Manufacturers who are planning to renew or sign new contracts with the Department of Defense (DoD) will be expected to meet the latest cybersecurity requirement later this year. The Cybersecurity Maturity Model Certification (CMMC), unlike previous DoD cybersecurity requirements which allowed for self-attestation, will require validation and certification by accredited third-party assessors. Manufacturers who plan to conduct business with the DoD will need to familiarize themselves with the CMMC requirements and prepare to comply.

Request for Proposals: This project will fund the evaluation and performance of CMMC readiness assessments for a select team made up of a medium to large size manufacturer and their supply chain(s).

Current Status: Proposals due July 30, 2020



Anticipated Period of Performance: 6 months

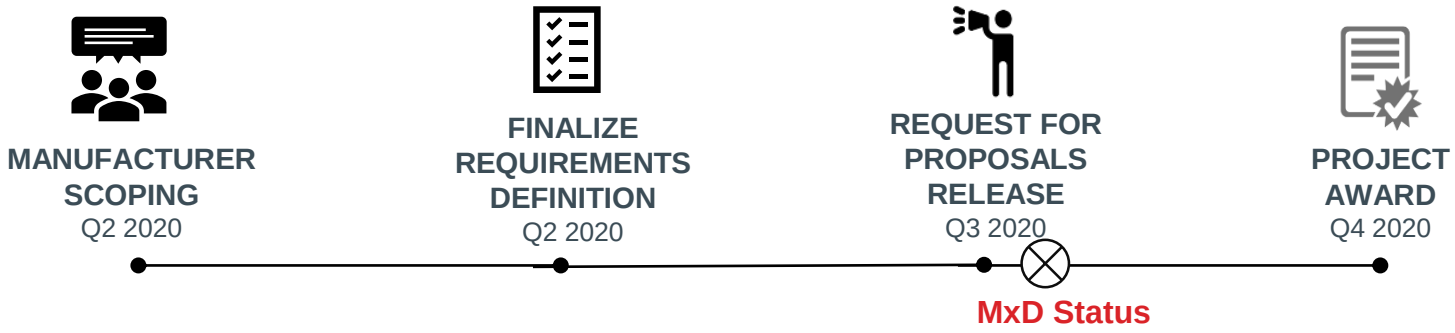
Anticipated MxD Funding: $100K - $150K

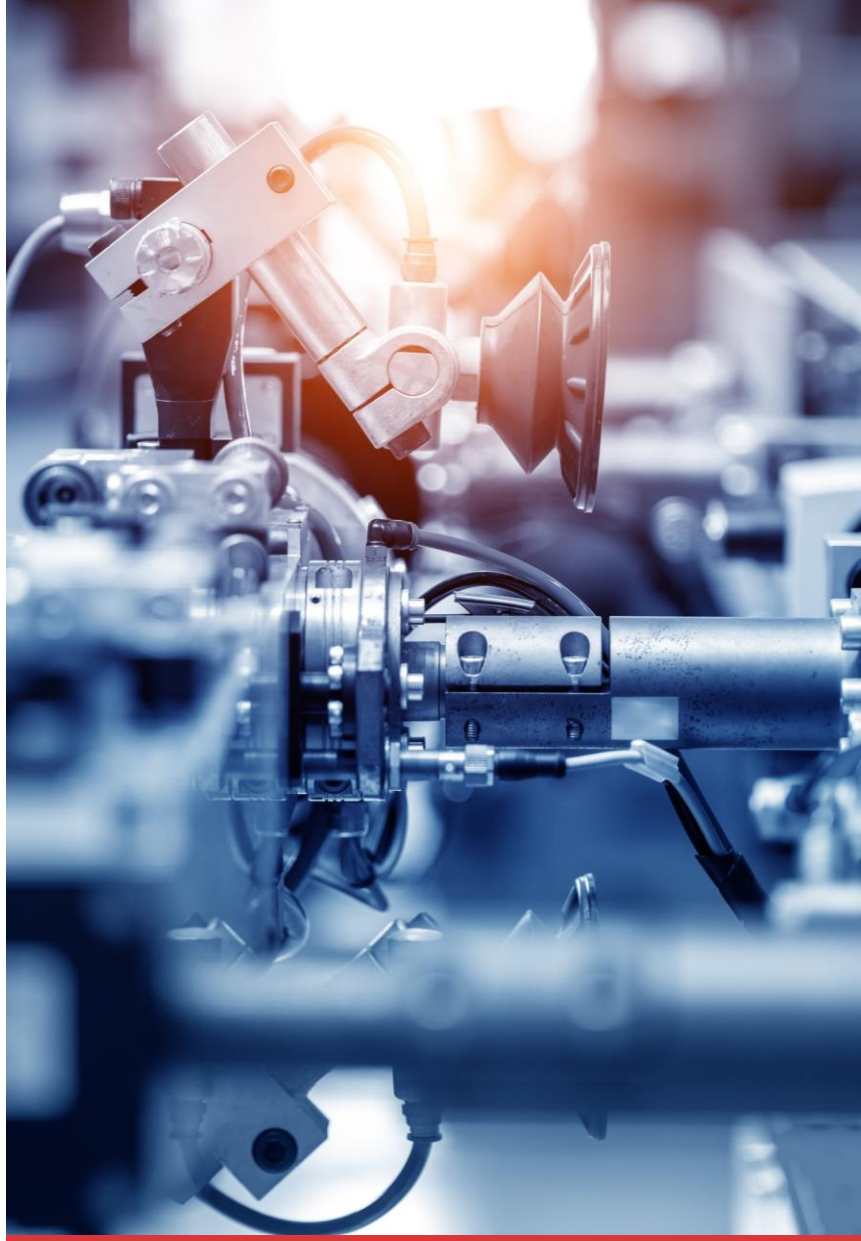
20-11: EMERGING TECHNOLOGY IN MANUFACTURING and CYBERSECURITY RESEARCH IN MANUFACTURING

Problem Statement: MxD plays an important role in connecting industry partners with the resources they need to better understand novel technologies that will have the highest impact to their businesses Through early engagement with industry stakeholders, researchers will be able to better structure their work to have maximum impact in the future. MxD is coming together with its industry partners to provide funding, guidance, and feedback for early stage, applied research in several different topic areas.

Request for Proposals: This project will fund multiple projects to support academic institutions in the furtherment of early stage (TRL 3-6) applied research in digital manufacturing and cybersecurity research in manufacturing.

Current Status: Proposals due September 3, 2020





Anticipated Period of Performance: 8 - 12 months

Anticipated MxD Funding: Up to $75K

CYBERSECURITY WORKFORCE PROGRAMS

Curriculum for High Schools and Community Colleges

- Collaborative development of high school curriculum with sister institutes America Makes and LIFT focused on “multi-skilled technician” skills. MxD developed high school capstone course focused on introduction of cybersecurity for manufacturing foundations for high school students.
- Working with local community colleges, MxD has worked to create a pathway to dual credit between high school courses and community college programs, as well as funding for apprenticeships to help

Virtual Curriculum – Cybersecurity for Manufacturing Operational Technology

- In partnership with University of Maryland – Baltimore County, a curriculum program designed to provide current workers with learning opportunities that result in certification(s), giving them the tools necessary to execute careers in cybersecurity in manufacturing and increasing the security of U.S. manufacturers from cyber attacks

Comprehensive Workforce Program for Cybersecurity in Manufacturing –Siemens Foundation Partnership

- In partnership with the Siemens Foundation, a comprehensive approach to workforce programs with cybersecurity in manufacturing, including the development of curriculum from middle school through postsecondary, job/role identification for careers in cybersecurity for manufacturing and hands-on learning opportunities through internships and apprenticeships

Manufacturing Education Engineering Program – Expansion of FlexFactor Program

- In collaboration with NextFlex and seven other sister institutes, MxD will lead regional implementation of the successful FlexFactor workforce education program
- The program, geared towards awareness building at the middle school level, will take a cybersecurity for manufacturing focus in the expansion led by MxD, helping students, teachers and parents understand the opportunities that exist for careers in cybersecurity for manufacturing

The Hiring Guide: Cybersecurity in Manufacturing

Purpose:

1. **Provides Cybersecurity in the Manufacturing Enterprise (Cyber^{ME}) job roles & career views to direct workforce decisions and investments by government, industry and company leaders, workforce developers and educators, and current and future cyber tech workers.**
2. **Deploys usable, key references to enable capabilities of small and mid-size manufacturers as well as larger industrialists.**
   - **Centralizes a current state view of Cyber^{ME}**
   - **Identifies pathways for transitioning and experienced workers.**
   - **Refreshes manufacturing industry supply and demand data.**
   - **Create shared view of the Cyber^{ME} talent ecosystem.**

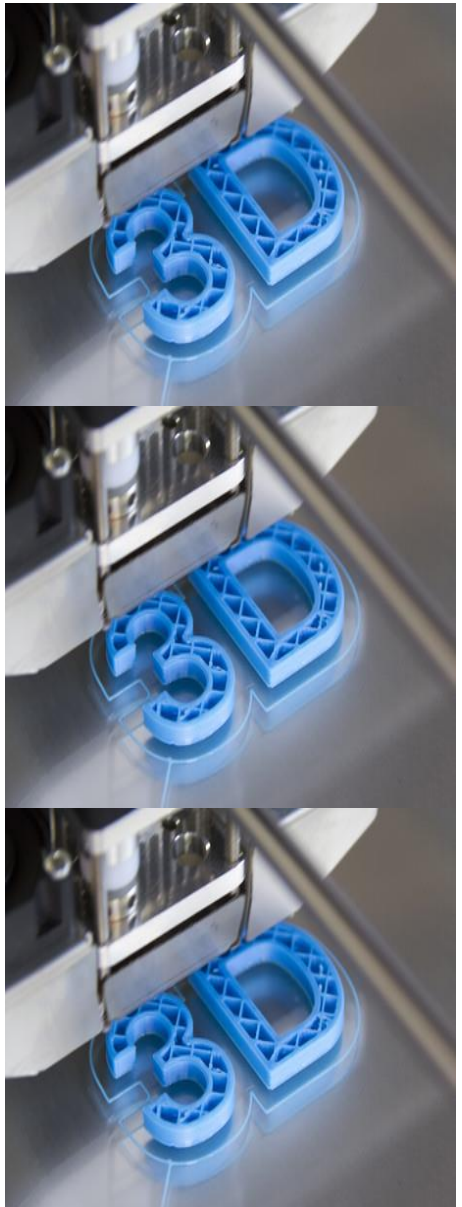
Primary Deliverables:

- **Cyber^{ME} Community of Roles**
- **Success Profiles of Key Roles**
- **Career Paths and Representative Personas of Key Roles**
- **Capability Adjacency Trends and Representative Personas (Report)**
- **Defining the US Ecosystem for Cyber Talent in Manufacturing (Call to Action)**

ADDITIVE MANUFACTURING RISK ASSESSMENT

Challenges:

- Security requirements are not clear in contracts for lifecycle management, including purchase and use of 3D printers
- Existing risk management frameworks are designed with data/information protection as a focus
- 3D printer manufacturers have not prioritized security as a requirement in the design and manufacture of their equipment
- Promised productivity improvements from use of equipment are not fully realized



ADDITIVE MANUFACTURING RISK ASSESSMENT

Established Scope for Phase 1:

- Machine-Level: How can the AM Machines be secured? This includes identifying gaps in making AM machines secure, implementing best practices, etc.
- Manufacturer Communications: How can these cybersecurity needs be conveyed to AM Machine Manufacturers/ Providers?

Assessment Framework/Approach:

- Develop risk profiles for AM equipment (3D Printers)
- Benchmark existing controls and practices against controls (instructions) in CNSSI 1253
- Identify and document gaps and related risks
- Recommendations on opportunities for addressing gaps and related risks
- Assess progress to compliance with CNSSI 1253 instructions
- Define implementation steps (pending review and approval of recommendations)

ADDITIVE MANUFACTURING RISK ASSESSMENT

Goals:

Determine a pathway to better secure and derive greater benefits from the deployment and use of 3D printer capabilities

- Greater understanding of risks and gaps for deployment and use of Additive Manufacturing equipment to established security controls in CNSSI 1253
- Develop repeatable best practices and related processes for a feedback loop between End-Users and equipment manufacturer
- Identify and recommend controls to address implementation risks and gaps
- Socialize and determine potential next steps for enhancements to secure AM deployment and use

Team composition:

A cross functional team of equipment manufacturer, solution providers, MxD and subject matter experts at military location(s) will work collaboratively to advance the goals of the assessment and define a path for implementation of the improvements to controls.

ADDITIVE MANUFACTURING RISK ASSESSMENT

Expected Deliverables:

- Assessment report
- System Security Plan
- Plan of Actions and Milestones
- Framework for continuous feedback (communication) between equipment manufacturers & users

Key control considerations:

- Access controls: Physical and logical access controls to printers, network and more
- Integrity checks: File integrity checks to guard against modifications to design
- Structural validation: Testing, inspection and validation of output for structural integrity
- Encryption for file/model protection: To ensure file content in wrong hands cannot be accessed or tampered with

National Center for Cybersecurity in Manufacturing

"Securing America's Supply Chains"

Federico Sciammarella
President/CTO, MxD

federico.sciammarella@mxdusa.org
office: (312) 281-6827 | **mobile:** (312) 927-0596