Cybersecurity and Industry 4.0

Federico Sciammarella

CTO, MxD

October 12, 2023

Manufacturing USA® Exists To Increase U.S. Competitiveness


M D
The Digital Manufacturing
& Cybersecurity Institute

US Manufacturing Industrial Base

239,607 U.S. MANUFACTURING FIRMS

178,210 Small Manufacturers
< 20 Employees

57,373 Medium Manufacturers
20 < Employees < 500

4,024 Large Manufacturers
>500 Employees

Source: https://www2.census.gov/programs-surveys/susb/tables/2020/us_state_6digitnaics_2020.xlsx

Manufacturing Industrial Base Impact to Economy

Contributes

24% of GDP

Employs

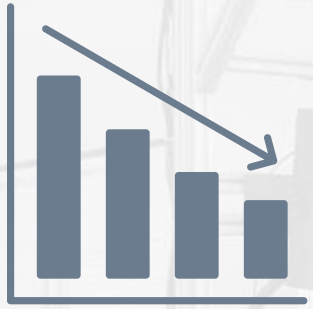
9.6%

Chemicals

#1 Sector

A resilient manufacturing base is critical to economic prosperity and national security

Manufacturing Industrial Base Is Facing Challenges

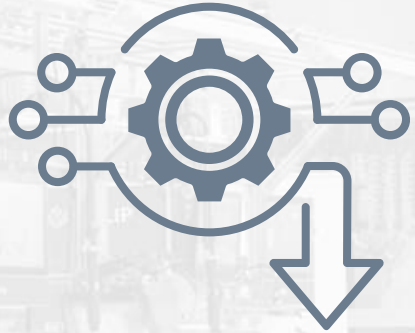


≈20k Lost

Industrial base is shrinking with **11% of the Smallest Manufacturers lost** in 10 years

#1 Target

Since 2021, manufacturing is the **top cybersecurity attacked industry**



2.1M Gap

U.S. manufacturing jobs expected to go **unfilled by 2030** due to a skills shortage

CONVENE THE ECOSYSTEM

ADVANCE TECHNOLOGY INNOVATION & ADOPTION

EMPOWER THE WORKFORCE

MxD Ecosystem
Collaborating to Drive Impact

DoD + Other Government

Manufacturers

Solution Providers

Academics

Non-Profits

THE INDUSTRY 4.0 LANDSCAPE

The Vast Majority of Manufacturers Are Small Companies

98% of U.S. manufacturers have fewer than 500 employees
73% of U.S. manufacturers have fewer than 20 employees (www.nam.org)

The 80/20 Rule at Major Companies

Many large companies only manufacture about 20% of the components in their products
You do not need to go too many levels in the supply chain to find a small business. See above!

There Are No Universal Standards for Digital in Manufacturing

There are a plethora of enterprise systems
Constantly evolving protocols with little interoperability
Continued wide use of vendor proprietary interface schemes

The Rate of Adoption of Digital Is Wide-Ranging

Varies by industry, region, and size of company

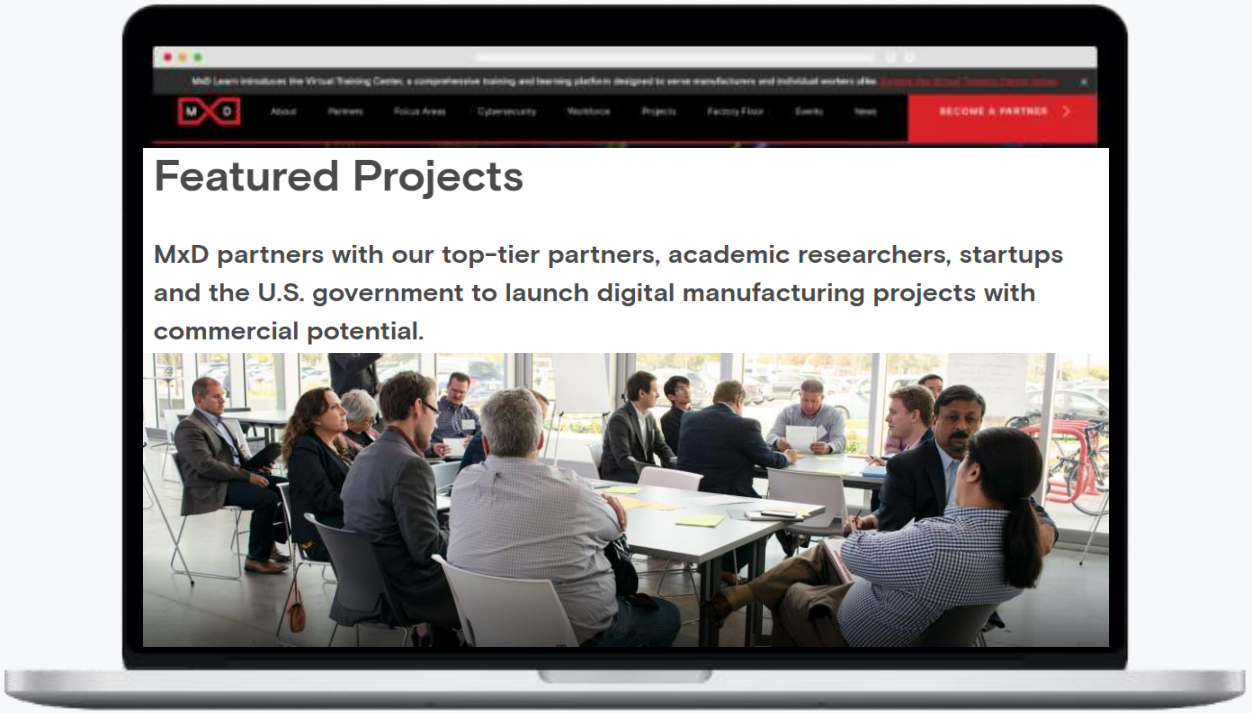
Cybersecurity must be part of digital transformation

There is no one size fits all approach


Design for Security
Incorporate cyber across people, design and process

MxD Projects

Collaborating with Members to Address Industry Needs



mxdusa.org/projects

23-11: Cybersecure Enclave Infrastructure as Code

Problem Statement: Small and medium manufacturers are not typically dedicated entirely to DoD production. These manufacturers do not have the resources to create secure networks for DoD cybersecurity requirements. This results in fewer manufacturers who can support DoD manufacturing priorities with increased operational costs to DIB/OIB suppliers who do comply with DoD cybersecurity requirements and leads to lowered competitivity of US manufacturing with an inability to realize opportunities of IT/OT connected enterprises.

Project Call: This project will create a configurable software architecture resource that small and medium manufacturers can use in their environments. MxD is soliciting proposals that address the need for a software solution targeted at small and medium manufacturers to simplify provisioning, deployment and maintenance of a secure network infrastructure for DoD manufacturing production.

Current Status: **RFP release September 14th, Proposals due November 9th**

Anticipated Period of Performance: 12 months

Anticipated MxD Funding: $600K

Q2 2023
PROJECT SCOPING

Q3 2023
DEVELOP PROJECT CALL

Q3 2023
PROJECT CALL RELEASE

Q2 2024
PROJECT AWARD

Notification of Participation by Foreign Firms & Non-U.S. Citizens

Membership in MxD shall be granted only to U.S. companies, firms, organizations, institutions, or other entities organized or existing under the laws of the United States, its territories, or possessions (as defined in Section 120.15 of International Traffic in Arms Regulations, 22 CFR § 120 et. seq. ("ITAR")).

Membership and project participation (or participation in projects without membership status) will be granted on a case-by-case basis at the sole discretion of the MxD Senior Leadership Team upon approval of the U.S. Government for any of the following:

- Any agency or instrumentality of a foreign government;
- Companies, firms, organizations, institutions, or other entities not organized or existing under the laws of the United States (as defined in Section 120.16 of the ITAR); and
- Non-U.S. Citizens.

In such event, all Members will be notified immediately of the foreign entity's role.

If a Member is a Corporation with subsidiaries or affiliates, its membership will include its wholly-owned and controlled and majority-owned and controlled U.S. subsidiaries and affiliates who qualify as a U.S. person under Section 120.15 of the ITAR.

It is a requirement that work related to the project must be completed in the U.S. by people legally authorized to work in the U.S. All proposed project participation by non-U.S. Citizens must be disclosed to MxD on Attachment 2c MxD Foreign Firms, Travel, & Non-U.S. Citizens at least 60 days prior to proposed participation. Written approval of foreign firms and/or non-U.S. Citizens must be received by the member of the Proposal Team from MxD prior to commencing work.

STRIDER

5.3B Documents Collected

3B Documents in Simplified Chinese

161M PRC Company Records

Continuously updating **10M** new docs per day

732M Resumes

35M Names analyzed

146M Patent filings from over **100** patent offices

248M Research articles from over **10K** publishers

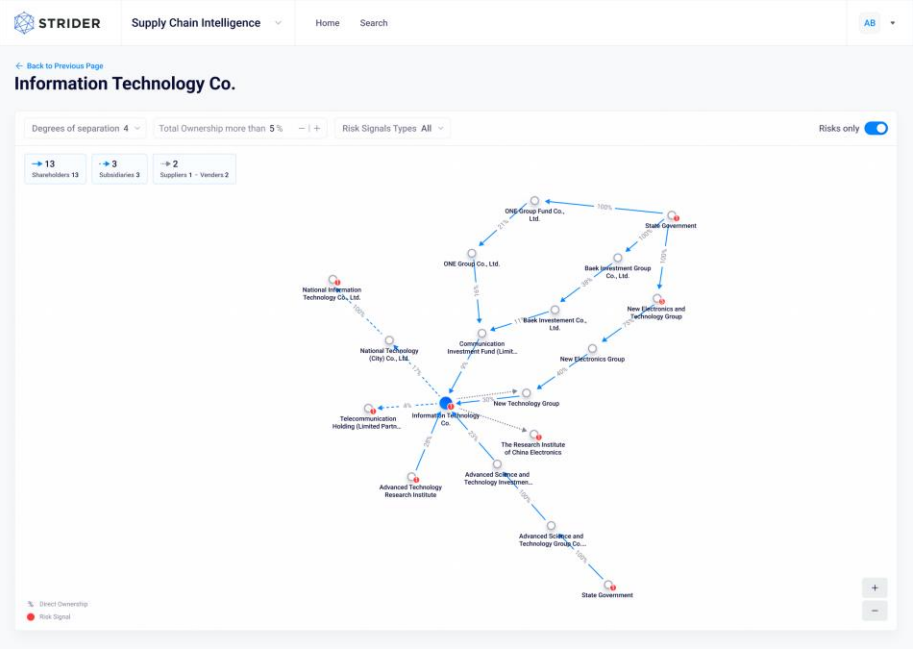


*Image from Supply Chain Intelligence

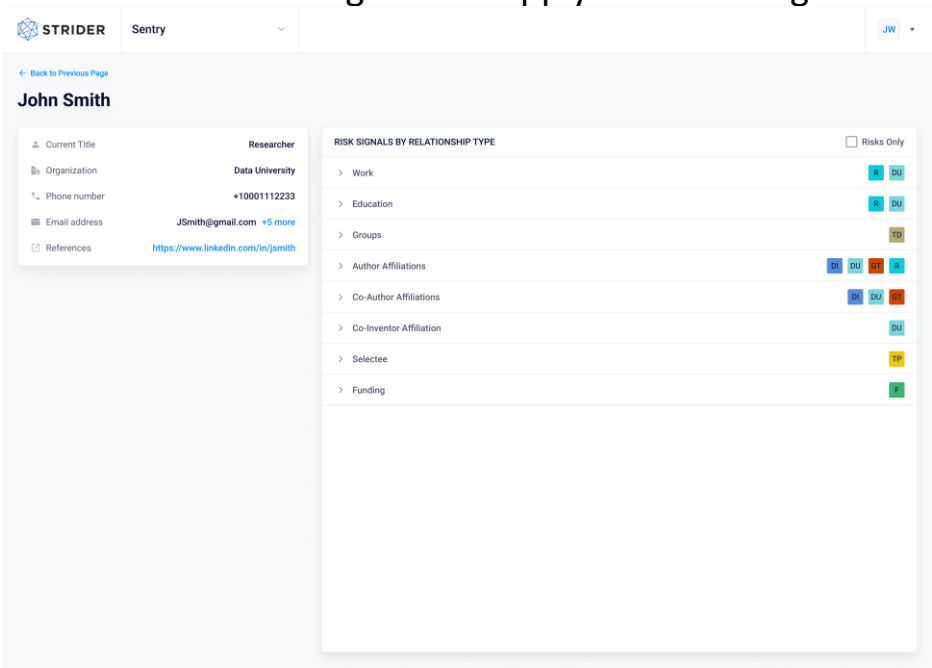


*Image from Sentry

Screen third-party entities (including other universities) for security risks before collaboration and partnership.

See if the entities are connected to sanctioned and restricted entities, military end users and suppliers, defense training and research organizations, and other state-owned entities.

Safely meet your talent needs by instantly illuminating potential connections to state-sponsored risk.

Instantly illuminate potential connections to state-sponsored risk for talent, partners, and collaborators.

MxD Learn

DEFINE | DEVELOP | DO

Identify the Future of Work

Create the Training Programs

Provide the Hands-On Learning

Led by Industry

Driven by Community

Focused on Under-Engaged

The Digital Workforce: Succession in Manufacturing

Hiring Guide: Cybersecurity in Manufacturing

Cybersecurity for Manufacturing Operating Technology Curriculum Program

Digital Design & Advanced Manufacturing Curriculum Program

DMCSPs and MEP Partnerships (NC, IL, RI, CT)

CAPITAL: Curriculum and Pathways Integrating Technology and Learning

MxD Learn Virtual Training Center (VTC) Platform

A white label, Open edX, virtual platform for recruiting, training, and securing the manufacturing workforce.

Workshops

Leveraging Technology to Increase Accessibility:
a look at how manufacturers can diversify their workforce and address manufacturing skills gaps

Cybersecurity for the Blue Economy:
a look at the intersection of water in manufacturing, cybersecurity, and workforce needs

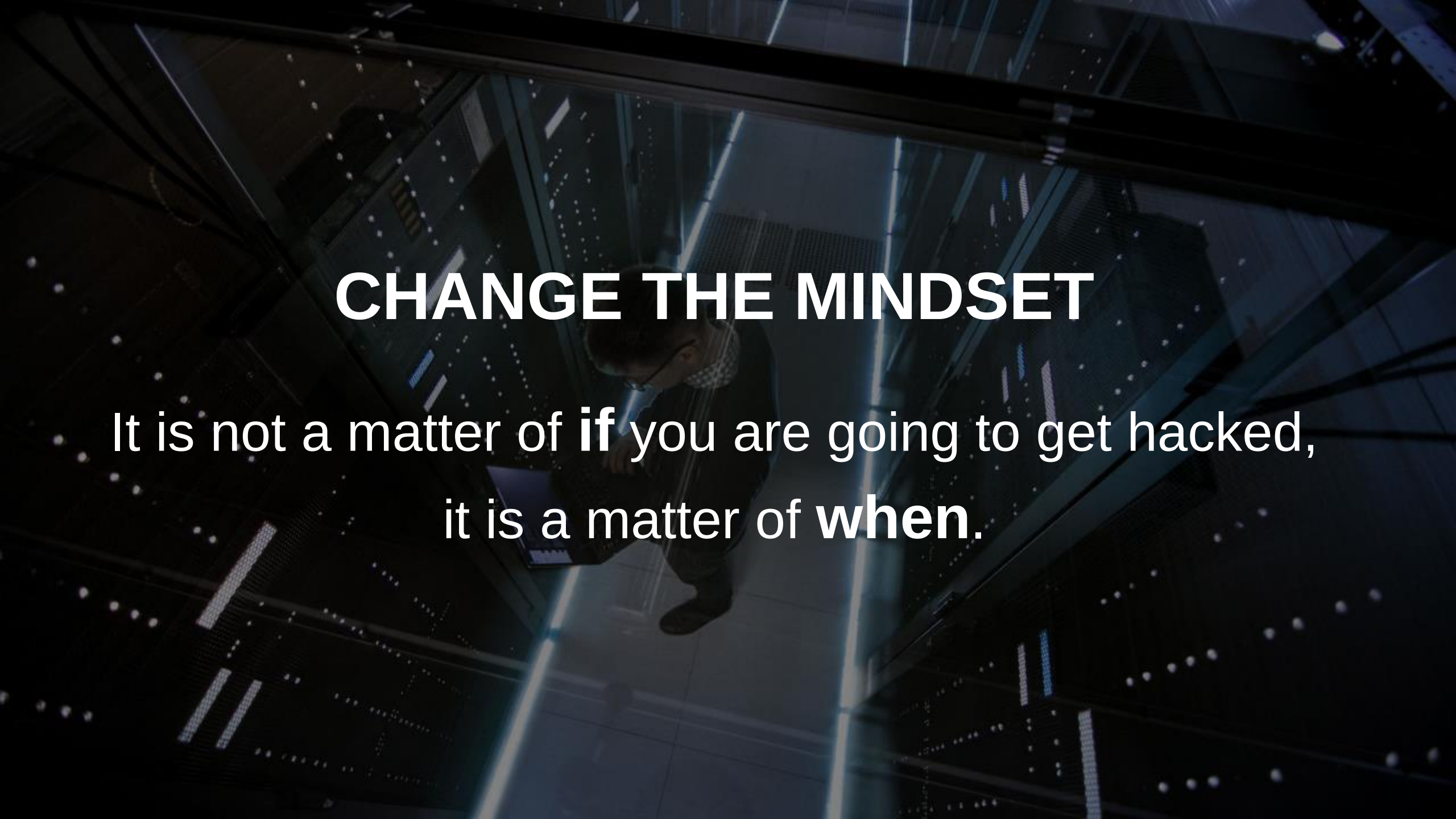
THE THREAT FOR MANUFACTURING IS INCREASING

#1 Since 2021, manufacturing has been the top attacked industry, with ransomware accounting for 23% of the attacks

61% of incidents at organizations with network connected operations technology (OT) were in the manufacturing industry

2,204% increase in reconnaissance against industrial controlled operations technology and software accessible by the internet

SOURCE: X-Force Threat Intelligence Index 2022, IBM Corporation, February 2022



CHANGE THE MINDSET

It is not a matter of **if** you are going to get hacked,

it is a matter of **when**.

MxD Cyber

National Center for Cybersecurity in Manufacturing

SECURING AMERICA'S SUPPLY CHAIN

AWARENESS BUILDING AND TRAINING

CYBERSECURITY TOOLS & SERVICES

CYBERSECURITY WORKFORCE PROGRAMS

SUPPORT STANDARDS COMPLIANCE

The Challenges Manufacturers Face

How do we scale without blowing the budget?

What standard should we use?

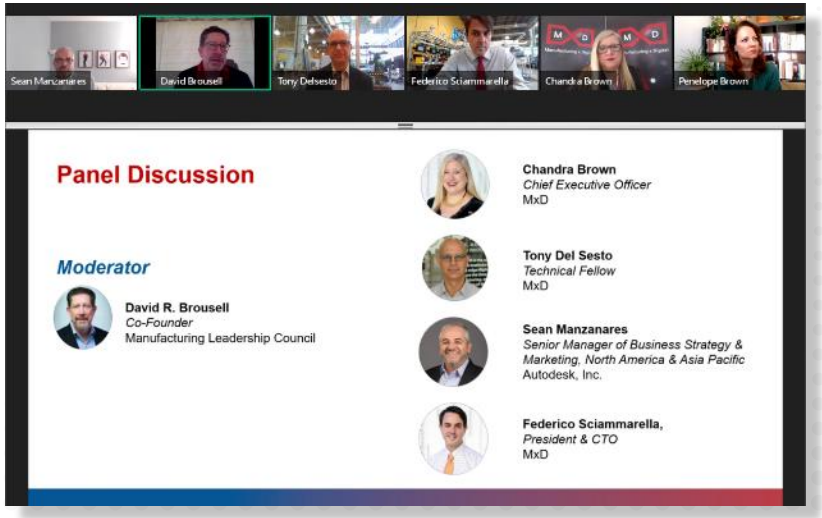
How do I manage all the tools and tech?

Where do we start?

Where do I find skills/talent?

10,000 Manufacturers Awareness Campaign
Stakeholders | Outreach

A. General



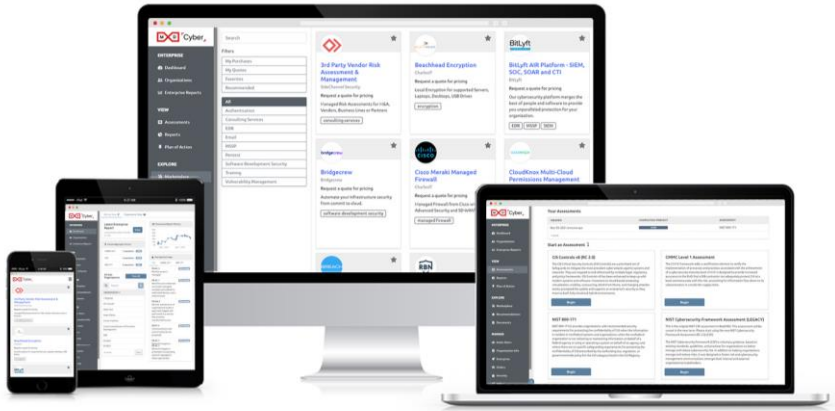
Webinars

B. Relevant

Roadshows, including MEP outreach

C. Engaged

Tabletop exercises

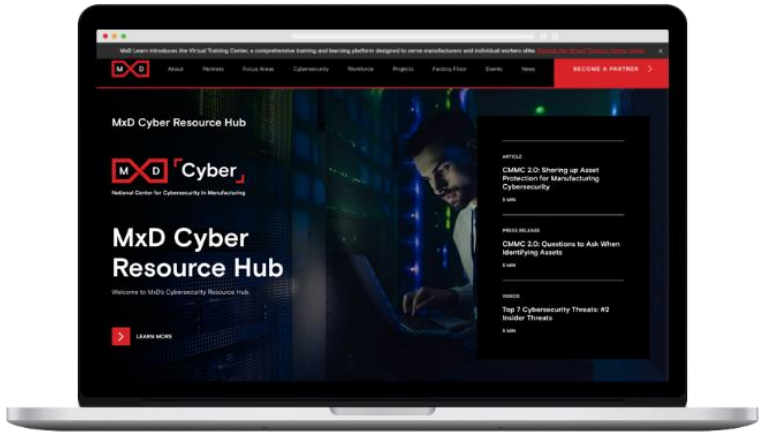


MxD Cyber MARKETPLACE

Cyber Assessments *Simplified*

- **MxD Cyber Resource Hub**

One-stop Resource for Cyber Content & Tools



mxdusa.org/cyber

Invite your supply chain on your digital journey

Rolls-Royce Supplier Cyber Program

Project Summary

This project was achieved through a partnership between MxD and Rolls-Royce, uniquely leveraging customer/supplier relationship to enhance the RR supply chain cybersecurity posture. Key components include awareness and educational content, hands-on workshops, and cyber assessments using the MxD Cyber Marketplace

Impact

MxD's efforts enhanced the Rolls-Royce supplier network by reaching 800+ RR suppliers with awareness/education content, CMMC assessments through the MxD Cyber Marketplace, and hands-on workshops and tabletops to enhance cyber preparedness

Project Participants

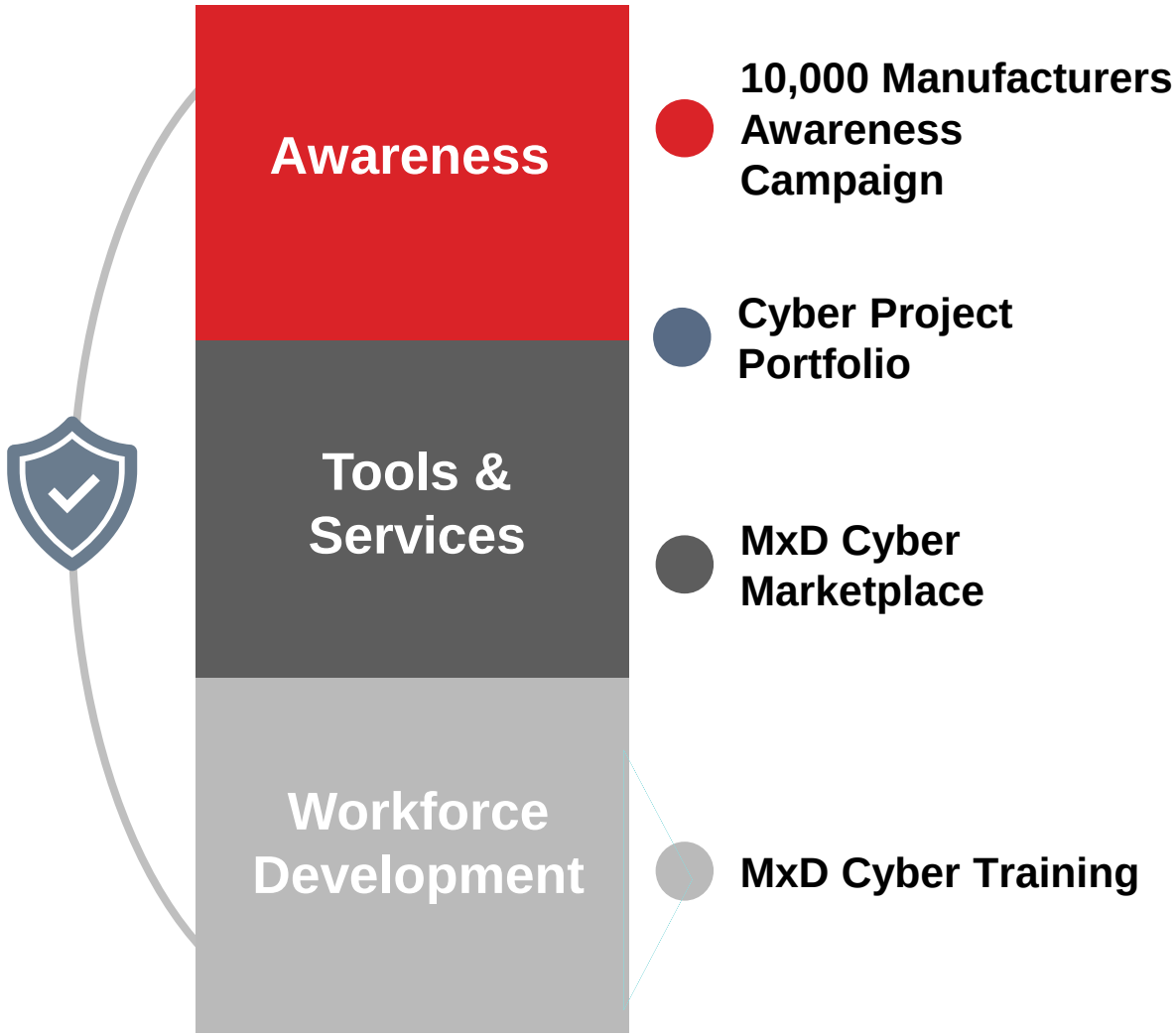
- Rolls-Royce
- 800+ RR suppliers

Rolls-Royce Supplier Cyber Program

MxD can understand the constraints that suppliers are under, especially small and medium sized manufacturers. MxD can provide tools, training, and guidance to help this population of suppliers. ***And ultimately, through the help of MxD, Rolls-Royce is able to reduce the cybersecurity risk within our supply chain.***

Neil Brink
Cybersecurity Specialist
Rolls-Royce

NCCM Impact in Progress



A repository of curriculum, tools & services, and factory floor implementations for securing ICS consumed by 100,000 audience members

50% of manufacturers who have been reached, adopted or accelerated cybersecurity implementations

Anticipate reaching 100 SMMs with Marketplace saving over $50k/year to enhance cyber posture

Reduce time costs required to undergo 3rd party assessments by 30%

80% of education related program participants have high sense of confidence in “next step” cyber hygiene implementation efforts

JDMC 2023

Keep up with all things MxD.
Follow us!

mxdusa.org

@MxDInnovates

/MxD

/MxDInnovates