

Cyber Awareness in Manufacturing: Building Competencies Through a No-Cost Digital Badge



Evelyn Brown - NC State University

November 14, 2023



The material is based upon work supported by the National Science Foundation under grant number 2000867. Any opinions, findings and conclusions/recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Presentation Outline

- ❑ Speaker Background
- ❑ NSF ATE Program/Project
- ❑ Cyber-Related Risks for Manufacturing
- ❑ Strategies to Lower Risks
- ❑ Cyber4RAM Digital Badge
- ❑ Cybersecurity Resources



Speaker Background

- Education
- Work in Manufacturing
- Work in Academia
- Current Role



NSF Advanced Technological Education Program

- ATE supports the education of technicians for high-tech jobs
- Involves partnerships between academic institutions, industry, and economic development agencies
- ATE funds support curriculum development, faculty development, and career pathway enhancement
- A list of active projects and links to related resources are maintained at www.atecentral.net

NSF ATE Project

Name: The Robotics/Automation and Cybersecurity Knowledge Sharing Coordination Network (TRACKS-CN)

Goal: Increase awareness among technicians working in manufacturing about the knowledge and skills required to maintain the infrastructure needed to operate connected machines in a manufacturing setting



TRACKS-CN Grant Partners

Community Colleges

Central Piedmont CC (NC)

Rowan-Cabarrus CC (NC)

Wake Technical CC (NC)

Spartanburg CC (SC)

Montcalm CC (MI)

Moraine Valley CC (IL)

Central Virginia CC (VA)

Bucks County CC (PA)

Marion Technical College (OH)

Lorain County CC (OH)

Gaston College (NC)

Manufacturing Extension Partnerships

NCMEP (NC)

GENEDGE (VA)

SCMEP (SC)

DVIRC (PA)

IMEC (IL)

MAGNET (OH)

MMTC (MI)

MEP at Columbus State (OH)

Other Organizations:

Digital Manufacturing & Cybersecurity Institute (MxD)

Advanced Robotics for Manufacturing (ARM)

NC Community College System (NCCCS)

National Initiative for Cybersecurity Education (NICE)



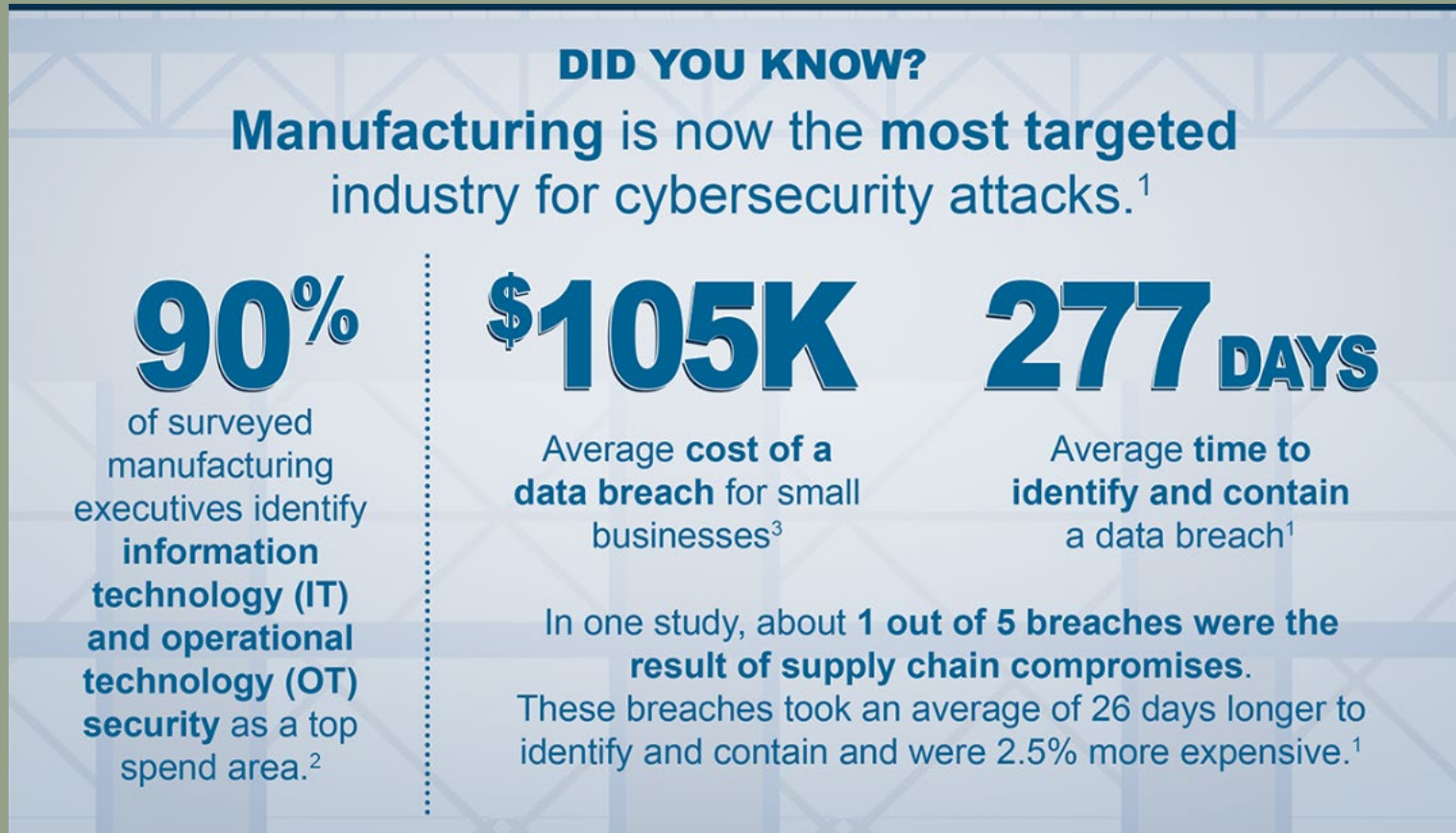
Manufacturing Extension Partnerships

- MEP National Network™ has centers that help small and medium-sized manufacturers survive and thrive.
- “... provides companies with services and access to public and private resources to enhance growth, improve productivity, reduce costs, and expand capacity.”
- “... interacted with 34,307 manufacturers, leading to \$14.4 billion in sales, \$1.5 billion in cost savings, \$5.2 billion in new client investments, and helped create or retain 125,746 jobs.”



Reference: <https://www.nist.gov/mep>

NIST MEP Infographic (10/27/23)



Reference: https://www.nist.gov/blogs/manufacturing-innovation-blog/infographic-integrating-cybersecurity-industry-40-what-it-means?utm_medium=email&utm_source=marketingcloud&utm_campaign=

Cyber-Related Risks for Manufacturing

- Operational shutdowns
- Loss of visibility over production and safety systems
- Financial loss due to outages and downtime
- Intellectual property theft
- Health and personal safety risks
- Denial of service

Source = Ty Middleton, CyMANII

Cyber-Related Risks for Manufacturing

- Significant unplanned costs for labor, overtime, idle equipment
- Increased or denied insurance
- Degraded equipment performance and quality
- Fees and lawsuits due to negligence or non-compliance
- Loss of ability to compete in the DoD supply chain
- Loss of customers

Source = Ty Middleton, CyMANII

Strategies to Lower Risks

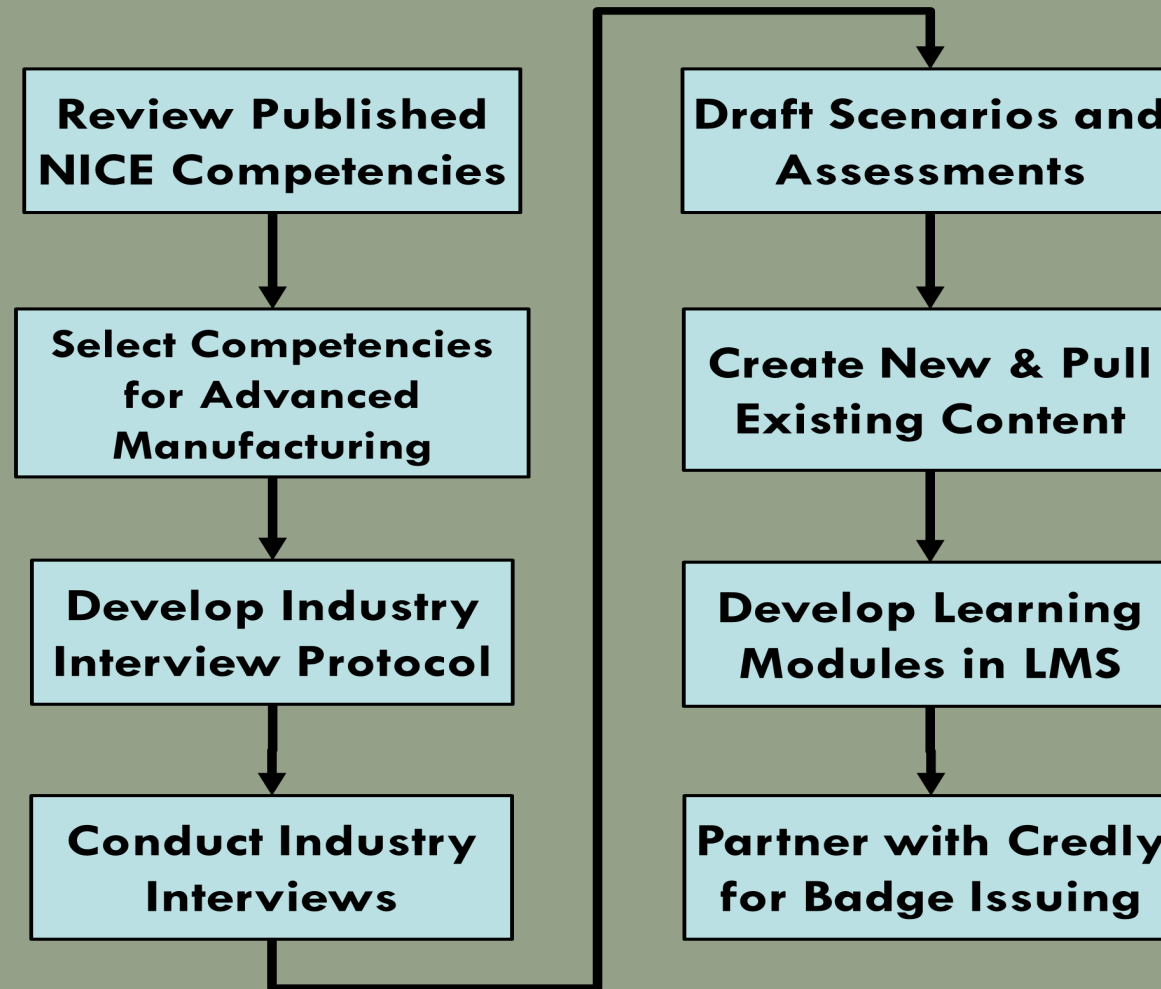
- Maintain and test an incident response plan
- Develop an access control policy
- Employ multiple authentication methods
- Remove unnecessary software/services and unused accounts
- Restrict remote access
- Provide cybersecurity training for all operators/administrators

Source = Ty Middleton, CyMANII

Cyber4RAM Badge

- A new micro-credential for technicians
- Goal: Provide technicians with content at the convergence of robotics/automation/mechatronics (RAM) and cybersecurity
- With manufacturers' shift to connected machines, their cyber-physical systems need protection
- Digital badges enable training content to be delivered outside of a classroom setting and at the learner's pace
- Workcred – <https://workcred.org/>

Badge Development Process



Cyber4RAM Badge Competencies

1. Asset and Inventory Management
2. Computer Languages
3. Data Privacy
4. Data Security
5. Digital Forensics
6. Identity Management
7. Incident Management
8. Infrastructure Design
9. Physical Device Security
10. Systems Integration
11. Vulnerabilities Assessment

Cyber4RAM Badge Website



TRACKS-CN Website (Badge Page)

Cyber4RAM Badge

A Digital Badge for Cyber Awareness

Our Motivation

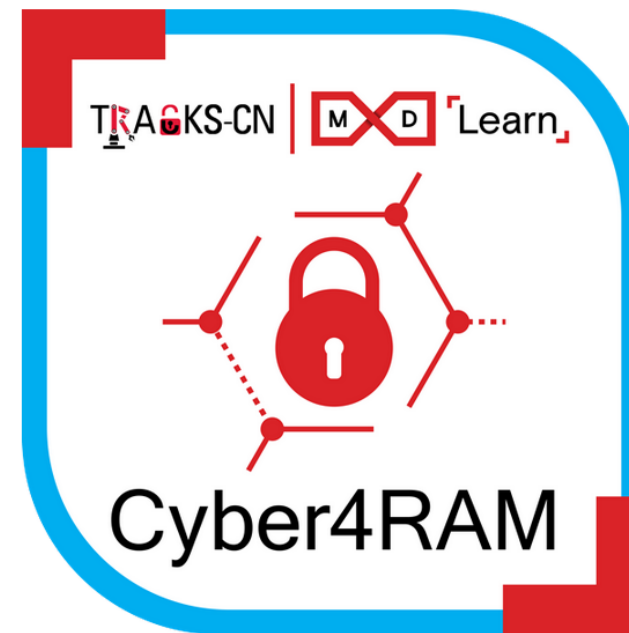
As more and more manufacturing facilities become connected, the likelihood that their connected equipment will be hacked increases. The TRACKS-CN team determined that a digital badge is an effective way to spread cybersecurity awareness to technicians within the realm of Operational Technology (OT) in robotics/automation/mechatronics (RAM).

Badge Competencies

The 11 competencies covered by the badge were selected from a list of 54 competencies published by the National Initiative for Cybersecurity Education (NICE). The 11 competencies tie to advanced manufacturing.

NICE Competencies for Badge

1. Asset and Inventory Mgmt.



**Enroll in TRACKS-CN Cyber4RAM
Badge Course**

Badge Demonstration

TRACKS-CN Cyber4RAM Level 1 Badge

Edit



Welcome to the Cyber4RAM badge, a badge designed to build awareness about cybersecurity among those who currently work or plan to work in the areas of robotics/automation/mechatronics. Since so many advanced manufacturing technologies are now connected, it is critical that technicians understand some cybersecurity basics in order to keep the machines they operate protected from outside threats.

Use the links below to navigate to more resources and information. You can use the Home link on the left side of the screen to return to this page.

[Purpose of this Course](#)

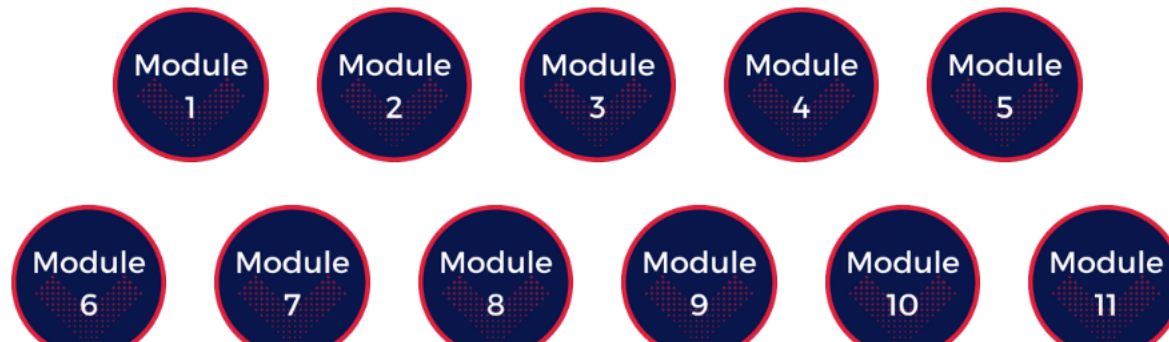
[Navigating the Course](#)

Badge Demo: Navigating the Course

Navigating the Course

This badge consists of 11 modules that explore essential cybersecurity concepts and apply them to robotics/automation/mechatronics in Advanced Manufacturing. Each module contains reading and video content, an example scenario, and assessment questions to allow you to demonstrate the knowledge that you have acquired. Upon successful completion of all 11 modules, you will be issued a Cyber4RAM Level 1 digital badge (through Credly) which can be placed on your electronic resume or professional social networking accounts.

To get started, click the **Module 1** button below. If you are returning to the course, click the next module that needs to be completed. Note that the modules **must** be completed sequentially.




Badge Demo: Module Overview

Module 1 Overview

Module 1: Overview

Module Summary

In this module, learners will be introduced to the processes of identifying, developing, operating, maintaining, upgrading, and disposing of assets.

The topics in this module align with NICE Competency 4: Asset and Inventory Management. More information about the NICE Framework may be found on the [NIST website](#) .

Learning Goals

1. Explain the purpose of asset management
2. Identify the distinct types of assets found in manufacturing
3. Explain the benefits of using an ITAM program for daily operations

Activities to Complete

Badge Demo: e-Mate Activity

Risk Management: e-Mate

Risk Management: e-Mate

One of the learning activities within this module relies upon the successful completion of an E-Mate. E-Mate Interactives help us learn difficult concepts. They were first developed under the leadership of Mike Quissaunee at the Brookdale Cyber Center and Dr. John Sands at CSSIA with funding from an NSF Grant (DUE 1601612). Please fully complete the activities within the interactive to help sharpen and develop your knowledge about cybersecurity.

The E-Mate for this unit is titled "**Risk Management**" and can be accessed through the following link:

http://e-mate2.s3-website-us-east-1.amazonaws.com/risk_management/risk_management.html 

To proceed, click the **Next** button. Each of the activities will require you to select **Mark as Done** before proceeding to the next activity. You can return to the homepage by clicking **Home** in the upper left corner.

◀ Previous

Next ▶

Badge Demo: e-Mate Activity

Risk Management Terminology

Introduction

Asset

Threat

Threat Agent

Vulnerability

Risk

Countermeasure

Security Control

Impact

Exposure

Risk Assessment

Risk analysis is a technique used to identify and assess factors that may threaten Information and Information systems. The study of Risk Analysis includes several commonly used terms.



Restart

3/7

Back

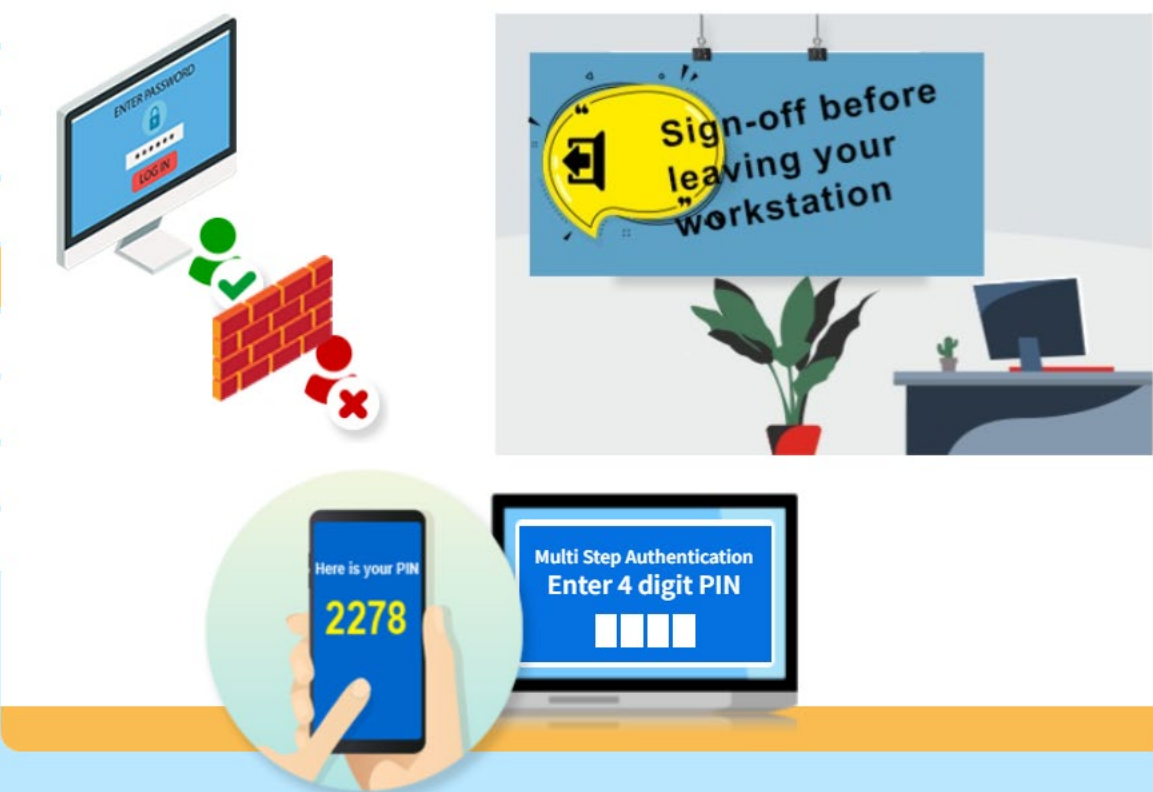
Next

Badge Demo: e-Mate Activity

Risk Management Terminology

- Introduction
- Asset
- Threat
- Threat Agent
- Vulnerability
- Risk
- Countermeasure**
- Security Control
- Impact
- Exposure
- Risk Assessment

An action, device, procedure, or technique that reduces a threat or a vulnerability by eliminating or preventing it.



The illustration shows a workstation with a sign that says "Sign-off before leaving your workstation". Below the sign is a laptop displaying "Multi Step Authentication Enter 4 digit PIN" with four input fields. To the left, a hand holds a smartphone displaying "Here is your PIN 2278". Above the laptop, a red brick wall with a red 'X' over it represents a vulnerability or threat, and a green checkmark over a computer monitor represents a countermeasure.

Restart 3/7 Back Next

Badge Demo: Module 1 Scenario

Module 1: Asset and Inventory Management

The Alpha Corporation produces industrial fasteners (nuts, bolts, washers, pins, clamps, etc.). In recent years, Alpha has invested heavily in upgrading its production capacity and the general modernization of their manufacturing environment. Much of the new equipment has been put into place without organization, asset tracking, or a formalized inventory system. As a result, leadership does not have an accurate up-to-date list of most of the equipment present within the facility.

As much of the equipment within the facility has started utilizing the Internet, management has experienced increased pressure to keep computers and equipment upgraded as many security patches are released each month. Currently, there is no formalized system for monitoring the updating/upgrading of company owned equipment.

Some of the manufacturing equipment has the ability to connect to the network directly through the use of an ethernet port. Currently, Alpha does not allow any lathes or mills to be attached directly to the internet, however this policy may have to change if the company wishes to install current patches from their vendors.

Badge Demo: Quiz Sample Question

Question 1

20 pts

Which of the following actions would be a prudent **first** step for management at Alpha Corporation:

- Acquiring a comprehensive inventory system to track company owned equipment and the equipments' status.
- Enforcing security gaps related to the asset's presence or configuration.
- Discover security gaps related to the asset's presence or configuration.
- Implement Biometric access to company owned equipment.

Cybersecurity Resources

- MxD - <https://www.mxdusa.org/>

The Digital Manufacturing & Cybersecurity Institute

- CyMANII - <https://cymanii.org/>

Cybersecurity for Manufacturing Innovation Institute



- NICE - <https://www.nist.gov/itl/applied-cybersecurity/nice>

National Initiative for Cybersecurity Education



Cybersecurity Resources

- NCyTE - <https://www.ncyte.net/>
National Cybersecurity Training and Education Center



- CSSIA - <https://www.cssia.org/>
Center for Systems Security and Information Assurance



- Cyberseek - <https://www.cyberseek.org/>
Resource for cybersecurity job market data

Cybersecurity Maturity Model Certification

- CMMC aligns to information security requirements of the DoD for partners in the Defense Industrial Base (DIB).
- CMMC is designed to enforce protection of sensitive unclassified information shared with DoD contractors/subs.
- CMMC provides the DoD greater confidence that contractors and subs are meeting applicable cybersecurity requirements.

Reference <https://dodcio.defense.gov/CMMC/about/>

Contact Information

evelyn_brown@ncsu.edu