Understanding and Improving Cybersecurity in Manufacturing

PI: Randall Sandone, UIUC

1 – Extended to all sectors
Project Overview

• Leveraging prior funding from DoD, develop, test, and sustainably transition to market a cloud-based SaaS application that:
  • Operationalizes the NIST CSF, Manufacturing Profile, and DoD CMMC
  • Supports SMEs, prime contractors, and entire supply chains
  • Delivers all references, best practices guidance, assessment tools, and POA&M
  • Supports embedded training
  • Complements other DHS tools, i.e., CSET & CDM
Approach

• Capability Gap Addressed: ability of organizations (govt. & commercial) and entire supply chains to quickly and affordably achieve compliance with cybersecurity standards and best practices
  • Gather and prioritize needs of end users
  • Engage with end-user groups to identify & prioritize industry needs
  • Identify and map NIST and DoD standards and best practices
  • Develop, test, and deploy accessible, affordable, easy-to-use SaaS application
  • Pilot test with end users
  • Execute technology transition plan
Testing, Evaluation, and Validation

• Software
  • All features, enhancements, and bug fixes are developed in separate branches
  • Every branch must pass a code quality check that includes conformity to development guidelines and software best practices
  • Every branch is tested by a minimum of two reviewers for functionality and usability
  • Multiple branches are tested in a staging environment before deployment
  • All code changes are tracked in an issue tracking system
  • An automated deployment system is used to create the testing environments and deploy the product
Testing, Evaluation, and Validation (cont’d)

• Organizational/Market Need
  • Conducted one-on-one needs assessments with small and medium-sized organizations
  • Interacted with industry user groups and organizations such as MxD and NIST MEP to identify and assess organizational needs
  • Engaged IBC to conduct market and competitive analysis
  • Conducted multiple pilot projects that included surveys, user assessments, and feedback
  • Consulted with multiple cybersecurity professionals
  • Presented our approach at workshops and academic, government, and industry conferences
  • In-depth meetings with government regulatory bodies (e.g., NIST) and government offices (including CISA) responsible for reviewing and assessing contractor compliance to the standards
  • Implemented functionality that is directly linked to government-mandated cybersecurity standards and requirements
Milestones and Accomplishments

• Achieved to Date:
  • Needs analysis completed
  • Core design and initial development & test completed
  • Manufacturing Profile integration completed
  • Market analysis completed

• Milestones Remaining:
  • Integration of embedded training in process
  • Integration of CMMC requirements in process
  • Go to market strategy in process
  • Engagement with DHS CISA, DoD and private sector in process
Project Impact

• Will improve the security and resilience of our nation’s critical infrastructure by:
  > facilitating a badly-needed shift to a more balanced approach to cybersecurity and resilience – nationwide
  > Improving cyber security postures and growth in maturity
• Will address capability gap at DHS CISA in addressing oversight of .gov domain compliance with EO 13800 – NIST CSF
• Will ease DoD contractor compliance with CMMC mandates
Despite higher spending on cybersecurity, costs due to cyber attacks continue to grow exponentially.
Where we are today:

Products & Technology

Process  People
Where we need to be:
Training-Augmented Dashboard

In-Context Training:
- Security Requirements
- Risk & Vulnerability Assessment
- Controls Implementation
- Monitoring & Mitigation
- Hands-on Training & Testing

Cyber Range

In-Class Training:
- Risk Awareness
- Risk Management Process
- Duties & Responsibilities
- Policies & Implementation
Process Powered by People -> Maturity:

Cyber Security Talent Management
- Education
- Experience
- Certifications

map

KSAs
- Tasks

Roles & Responsibilities

Training

update

map

Requirements Controls

Cyber Secure Dashboard

Training Delivery
Technology Transition

• End-Users
  • Governance, Risk Management and Compliance (GRC) tool
    • Small and Medium Enterprise
  • Educational tool
    • Via integration to a learning management systems (LMS)

• Self-Sustainability Strategy through Rangerfish, LLC
  • Independent commercialization entity
  • Consolidated IP Rights from inventors and UIUC
  • Control of future R&D in partnership with UIUC and HSTG
  • Provides continuity to project by following CIRI-developed strategy