Course Title: Cybersecurity: An Introduction for the Automotive Sector

Course Length: 1 day, in-person

Time in Class per day (hours): 8 hours of in-person instruction

Delivery Options: Company site or at provider

Class Size: Minimum 8 / Maximum 25

Price Per Student: $1,195.00

Location: Wayne County *or* Company Site

Course Description:

The automotive industry is the new "battleground" for cybersecurity. Following the path of desktops/laptops, tablets, and mobile phones, the automotive industry is now the "hot" area for both academic researchers and hackers. This will transform the automotive industry just as it transformed traditional information technology and the mobile markets; it is inescapable, but it can be beneficial and a well-prepared company can find significant benefit in being a market leader.

What does cybersecurity mean? Who is attacking and why? What must we change? What can stay the same? What is the larger organization's role in cyber? What will the government likely do and how will it affect us? Are there measurements - what does "secure" look like? These questions and more will be answered by this seminar.

We live in an age when cyber-related recalls will happen, when remote, over-the-air updates will become routine, and in which our cars have more lines of code than a small office. This seminar introduces critical cybersecurity concepts and puts them in an automotive context. It cuts through to the "so what" basics that enable understanding and provides ideas to implement in your company. Interaction and discussion is important, so after each lecture block there is a discussion period and a written work product.

Course Learning Objectives:

Upon completion of this course participants will be able to:

- Describe key concepts in automotive cybersecurity such as the InfoSec Triad; Threat, Vulnerability, and Risk; Defense in Depth, etc.
- Understand the importance of organizational roles and support, and how doing this can make cybersecurity an operational value proposition and not just a costly after-thought
- Understand and recognize good software and embedded security practices
- Understand why "hackers" are focusing on the automotive industry, and how they tend to think and operate.

Michigan Alliance for Greater Mobility Advancement

Course Content/Syllabus:

Introduction
- Definitions
- Vulnerability
- Threat
- Risk
- TARA (Threat Assessment and Remediation Analysis)
- Architecture
- Attack classes
- State of the Standards (SAE, NIST, ISO)

InfoSec Triad - "Plus"
- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Apply to automotive
- Discuss critical design features (e.g. availability vs integrity)

InfoSec Governance
- Standards
- Roles and responsibilities
- Ongoing monitoring
- Oversight
- Value

Secure Software Development
- Scope/scale of problem
- Proper design of software quality assurance/testing
- Continuous integration
- Evaluation of 3rd party code
- Techniques (e.g. overflows, data protection, etc.)
- Cryptography

The Adversary - Hackers
- Changing demographics, motivation, and identity
- Work process (e.g. flash dumping dynamic analysis, etc.)
- Case study

Embedded Security
- How embedded security differs from “traditional” security – pros and cons
- Embedded hardware lock-down
- Key software development for embedded systems

Diverse Topics
- Overview of some hardware and software cybersecurity techniques and products

- Resiliency
- Supply chain cybersecurity
- Understanding built-in vs bolt-on argument and how to evaluate efficacy
- Defense in depth
- Stepping through an exemplar layered system

MAGMA short courses are held on a rolling basis, based on industry demand. Please complete this **short form** to express interest for yourself, or your organization.