Advancing Cybersecurity Programs: Lessons from TARA Process Evaluation

Urban Jonson

IOActive.

Urban Jonson, CISSP

Current

- Technology and Cybersecurity Advisory
- US FBI InfraGard Transportation Subject Matter Expert
- FBI Automotive Sector Specific Working Group (SSWG)
- Secretary - Board of Directors, Cyber Truck Challenge
- Program Committee, ESCAR USA
- SAE Vehicle Electrical System Security Committee Member
- Technology & Maintenance Council (TMC) S.5 and S.12 Study Group Member

Experience

- Over 35 years of experience in IT and cybersecurity, including strategic planning, assessments, project management, and program management
- Various papers, talks, and research on hacking, as well as defending trucks and transportation in general
- Abusing and defending systems since the 1980s

IOActive.

Agenda

- Framing the Challenge
  - Governance, ROI, and program efficacy
- TARAs as a Case Study
  - How Threat Analysis and Risk Assessment reveal strengths and weaknesses
- Survey Insights
  - Key findings from OEMs, suppliers, regulators, and fleets
- From Compliance to Value
  - Turning TARAs into safety-critical, value-driven processes
- Process Improvement
  - Lean, Six Sigma, and governance alignment
- Program Improvement and Optimization
  - Path forward to faster, smarter, cost-effective cybersecurity

Why this topic?

Governance and Costs

- Increased focus on good governance in cybersecurity
- NIST Cyber Security Framework (CSF) 2.0 specifically calls out governance
- With governance comes policies and procedures
- How well do your cybersecurity operations align with governance?
- Increased pressure to reduce costs and streamline security operations

Program Efficacy and ROS/ROSI

- Cybersecurity programs are costly — but are they effective?
- Many organizations grow organically, creating inefficiencies
- Without clear measurement, it's hard to know:
  - What's working?
  - Where waste exists?
  - How to justify investments?

Let’s Look at an Example

Threat Analysis and Risk Assessment (TARA)

Threat Analysis and Risk Assessment Study

- Interview industry stakeholders about their use of TARAs
  - ✓ OEMs
  - ✓ Tier 1 Suppliers
  - ✓ TARA Tool Providers
  - ✓ Industry Experts
  - ✓ Regulatory Authorities
- Look at tactical execution versus the theory
- Determine if TARAs are treated as a living critical safety artifact, a check-box compliance nuisance for type approval, or something in between
- What are the process issues, if any?
- How can we improve existing processes

IOActive.

TARA overview

What is a TARA?

What is a TARA?

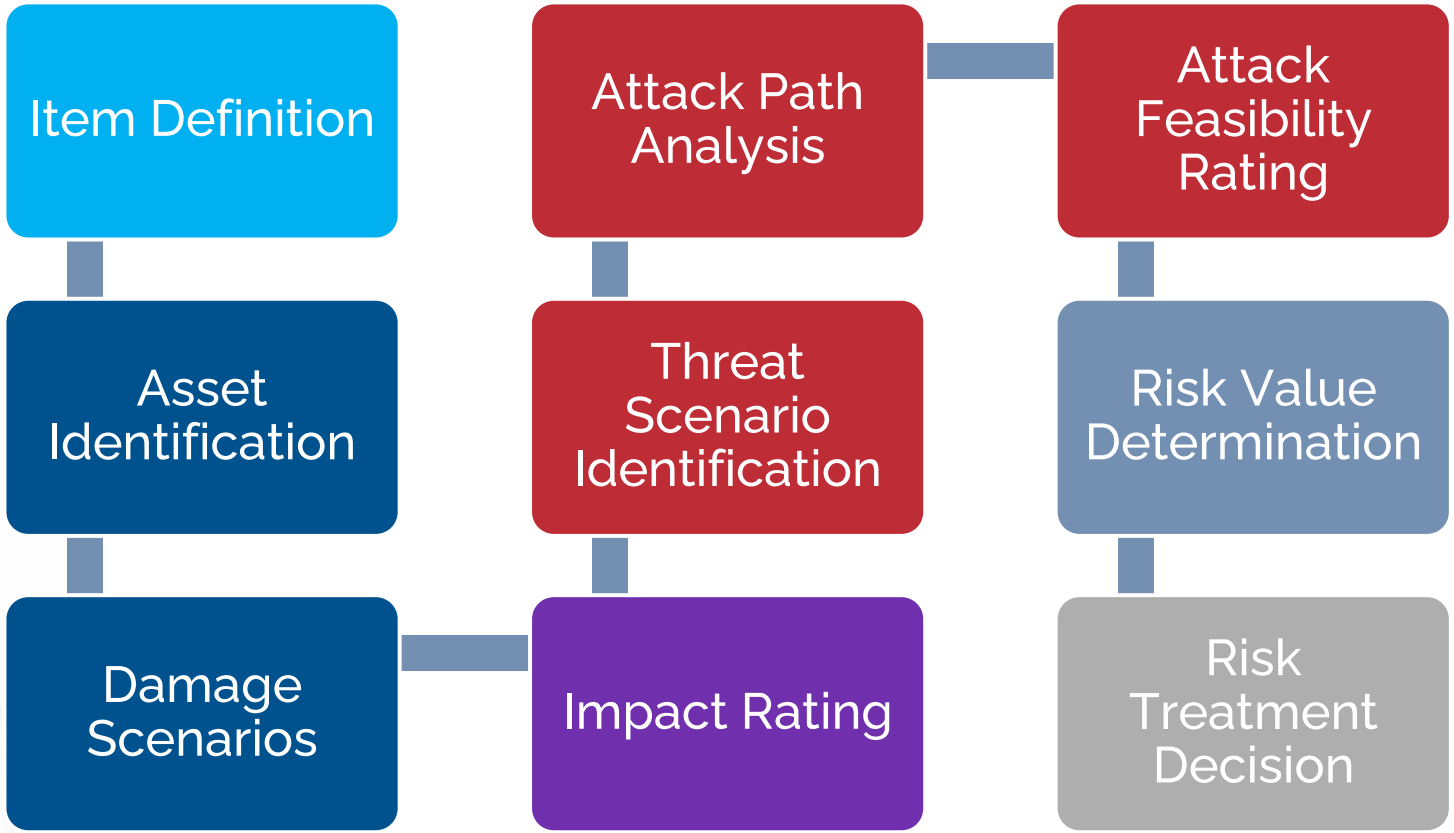
- Threat Analysis and Risk Assessment (TARA)
- TARAs are a type of threat model
- Initially conducted during the design phase of product development
- Conducted from the **attacker's point of view**, which requires an understanding of adversaries, different attack paths, and the feasibility of attacks
- Commonly used within ISO/SAE 21434 - Road Vehicles - Cybersecurity Engineering

What is a TARA?

- Unlike penetration testing, which is focused on a completed product
- Similar to architectural risk analysis
- Specific steps vary depending on the approach and models used
- Can help identify critical areas and components for third-party pen testing

IOActive.

ISO/SAE 21434 TARA process



Item Definition | Assumptions | Assets | Damage Scenarios | Threat Scenarios | Risks Analysis | Risk Treatments

IOActive.

TARA Steps (ISO/SAE 21434)

- **Item Definition**
  - ✓ Boundaries, functions, preliminary architecture
- **Asset Identification**
  - ✓ Data and functional assets, cybersecurity properties (CIA), damage scenarios
- **Impact Rating**
  - ✓ Rates the impact of the damage scenarios (Major, Severe, etc.)
  - ✓ ISO/SAE 21434 Annex F – *Guidelines for impact rating*
- **Threat Scenario Identification**
  - ✓ STRIDE, attack trees, PASTA, DREAD, known vulnerabilities (CVEs)
  - ✓ UNECE R155 Annex 5 – *List of threats and corresponding mitigations*

TARA Steps (ISO/SAE 21434)

- **Attack Path Analysis**
  - ✓ Routes or paths for exploitation
  - ✓ Requires an attacker's mindset
- **Attack Feasibility Rating**
  - ✓ Required knowledge, resources, time, and effort
  - ✓ ISO/SAE 21434 Annex G – *Guidelines for attack feasibility rating*
- **Risk Value Determination**
  - ✓ Combination of risk impact and feasibility
- **Risk Treatment Decision**
  - ✓ Reducing, mitigating, or accepting the risk

Process Take Away

- TARA process and methods can vary by organization
- There are ambiguities in every TARA process and approach
- Artifacts and deliverables can be organized in different ways and contain different information
- By their nature, TARAs are very subjective, and experience matters
- There is room for significant variation across large organizations with multiple product groups and varying levels of competence
- How to ensure TARA is a “living document” is not included in any guides

Why TARAs Matter for ROI & Governance

- TARAs bridge technical risks to business governance
- Done well:
  - Improves consistency → reduces rework → lowers costs
  - Strengthens type approval confidence
  - Enables risk-informed resource allocation
- Done poorly:
  - Becomes a “checkbox” exercise
  - Creates expensive paperwork, little risk reduction

Survey Results & Prespectives

"It is a journey"

Interview Targets

- OEMs
- Tier1 Suppliers
- Cybersecurity Experts
- Tool Providers
- Regulators
- Trucking Fleets

OEM Observations

- TARA process maturity varies substantially across OEMs, even the big ones
- TARAs are not always used in conjunction with ISO/SAE 21434
- Supplier agreement maturity varies significantly between OEMs
- The most significant variations or issues seem to be incorporating TARA information from and with suppliers (SBOM/HBOM)
- Most have a regulatory group that interacts with regulatory authorities for R155 type approval – either lawyers, engineers, or a mix of both
- People who create and maintain TARAs rarely interact with regulatory authorities

IOActive.

Tier 1 Supplier Observations

- Great variance in maturity between various Tier 1 suppliers
- Tier 1 suppliers tend to be less mature than OEMs, but not always
- Some are ISO/SAE 21434 “compliant,” but many are not since they only supply parts
- Some Tier 1 suppliers have supplier interface agreements, but many do not; instead, they use more traditional supplier agreements
- SBOMs and HBOMs are starting to become prevalent

IOActive.

Cybersecurity Expert Observations

- TARAs take longer and cost more than the client thinks they should
  - ✓ Lack of item or product documentation
  - ✓ Explore more attack paths than an internal team
  - ✓ Have a well-documented and specific process and deliverable templates to produce consistent and high-quality results
  - ✓ Processes are usually more comprehensive due to experience in multiple types of embedded systems
  - ✓ Extensive knowledge of vulnerabilities and cutting-edge hacking techniques
- Performing a thorough and high-quality TARA is laborious and tedious work, which causes project staffing challenges

IOActive.

Tool Provider Observations

- Majority of prospective customers use spreadsheets
- Fighting for budget is still an issue
- EU market is showing higher motivation than US market due to R155
- US and Asian markets are proving more difficult
- Tool providers are the only group that mentioned Auto-ISAC threat matrix

Tool Provider Observations

- Integration with existing engineering processes with unique tool chains is an ongoing learning experience for everyone
- Focus on moving to dynamic environments for “living documents”
- Large item definitions yield large spreadsheets with too much complexity
- Features include dashboards, automated attack trees, reports, alerts, and many other features to manage complexity across the enterprise

IOActive.

Tool Provider Observations

- Providing integration with SBOM/HBOM and reported vulnerabilities
- Integrating direct support for UNECE R155 Annex 5 – *List of threats and corresponding mitigations*
- Looking at advanced solutions like direct Ghidra support, which seems bleeding-edge
- Functionality across vendors varies, and customers should consider all major vendors to find the best fit for their organizations

IOActive.

Regulatory Authority Observations

- First priority is to evaluate company processes, Cyber Security Management System (CSMS)
- Review TARA process and validate TARA output
- Check to ensure the risk profile is maintained over time
- The TARA must be a living document
- Challenges with incremental changes, as there are no set rules for when to require a new type certification
- Heavy vehicle type certifications are complicated by the flexibility of vehicle configuration; focus on the most complex configuration
- Try to tailor the approach based on product and type

Regulatory Authority Observations

- Issues observed by the authority
  - ✓ Over-classification -> impact too high
  - ✓ Only looking at Annex 5 -> scope should be broader
  - ✓ TARA is subjective, resulting in varied quality
  - ✓ Tools vs Excel spreadsheets -> regulator/audit access
- Review CSMS every 3 years or so
- Tweak type approvals for type extensions
- Looking for updated TARAs when looking at extensions
- Looking for risk management, i.e., mitigated, transferred, and accepted
- At the end of the day, it is about handling risk

Trucking Fleet Observations

- Most commercial fleets are only marginally aware of ISO/SAE 21434 or similar standards or regulations, such as UNECE R155 and R156
- Cybersecurity awareness and posture vary significantly across the industry and types of fleets
- Assessments at vehicle build stage through paper and factory pilots and second-market evaluations
- TARAs could be useful, but are not employed
- Heavy-vehicle OEM customer education opportunity

IOActive.

Organizational structure

Different approaches

Organizational Structure

- **Distributed**
  - ✓ Engineers at the component/product level perform the TARA function
    - ✓ May or may not include cybersecurity training or certification
  - ✓ Specialized cybersecurity staff assigned to the component/product team perform the TARA function
- **Centralized**
  - ✓ Centralized team, develops and maintains TARAs for the entire organization, and works on multiple components/products at a time
- **Disorganized**
  - ✓ Organization is in the early phase of incorporating TARA into the development lifecycle, and no formal organizational structures exist

Organizational Structure

- Numerous approaches were employed to review output and ensure quality assurance
- In the best cases, peer review was followed by senior expert and management review and sign-off
- In the worst cases, there were few, if any, peer or formal review processes
- There is no guidance on developing a quality TARA process in any of the supporting documentation
- Best-practice quality assurance business process methods are not always applied in cybersecurity environments

Organizational Structure

- The amount of time required to complete a TARA depends significantly on who is doing the work
- External cybersecurity professionals take about 4 to 8 weeks for a TARA, depending on the size and complexity of the assets
- Internal staff take about 2 to 4 weeks to complete a TARA
- Internal staff have the benefit of inside knowledge, and external professionals tend to take a deeper dive and consider more attack paths and scenarios
- Most organizations perform TARAs internally, but a few engage external experts for more complex items

IOActive.

Common Issues

Common Issues

- TARA consistency seems to be a common issue across the supply chain
  - ✓ A factor of processes, assumptions, and deliverables
  - ✓ Lack of scaffolding, e.g., process documentation, templates
- TARA accuracy, especially impact assessments, also seems to be a common issue across the entire ecosystem
  - ✓ Assumptions, experience, and cybersecurity “know-how”
- Mixed tool and manual documentation
- Little or no document management support or document management systems

Common Issues

- Varying levels of training and expertise
- Little or no documentation or examples
- Sharing TARA information across the supply chain from “Tier *n*” to the regulatory authority seems challenging
- Mismatch and inexperience in supplier interface agreements
- New technologies such as EVs cause additional supplier and interface agreement issues

IOActive.

Conclusion

Safety-critical process or check-box compliance?

Conclusion

- There are many ways that TARAs can be implemented and supported
- Not everyone is using ISO/SAE 21434 to meet R155 compliance, but some still use TARAs as part of the development lifecycle
- TARAs are mostly taken seriously as part of safety-critical systems
- A few minor suppliers consider it to be check-box compliance because they have little to no connectivity
- Adoption and integration of TARAs is a journey that is specific to the company, and processes should be reviewed and updated regularly
- Everyone seems to have issues with quality and consistency

IOActive.

Issues Cause an Impact

- Frequent rework and corrections
- Poor integration with suppliers and regulators
- TARAs are not updated → outdated risk assumptions
- Increased compliance and legal risk
- Result: wasted resources, delayed approvals, increased spend, reduced ROI

IOActive.

How To Improve TARA Process

How to Improve

- Review existing processes
- Empower the person conducting the TARA
- Support the person conducting the TARA
  - ✓ Process documentation with complex and robust examples
  - ✓ Tools and document management systems
- Implement quality control processes and criteria
- Improve training across the organization, including engineering, purchasing, legal, etc.
  - ✓ Training providers exist, including SAE and UL/Kugler-Maag
- Get process metrics: *"If you can't measure it, you can't improve it"*

Process Improvement

Lean

- Focuses on eliminating waste (non-value-added activities) to improve efficiency
- Emphasizes continuous improvement (Kaizen) and empowering employees to identify inefficiencies
- Tools include value stream mapping, 5S, and Just-In-Time (JIT) production
- Goal: streamline workflows, reduce cycle times, and increase customer value

Six Sigma

- Focuses on reducing variation and defects in processes through data-driven methods
- Uses DMAIC (Define, Measure, Analyze, Improve, Control) as a structured improvement cycle
- Employs statistical tools to identify root causes and ensure process stability
- Goal: achieve near-perfect quality (x defects per million)

IOActive.

Process Improvement

- Identify the process
- Map the current process
  - ✓ Business process model and notation (BPMN)
- Analyze the process
  - ✓ Root cause analysis, value-add or not, cycle time, and wait time tracking
  - ✓ Define key performance indicators (KPIs) to measure the process
  - ✓ Determine error rates, rework, tasks, and effort at each stage of the process
- Identify possible improvements
  - ✓ Eliminate waste, simplify hand-offs and approvals, standardize tasks
  - ✓ Add automation and tool support

Process Improvement

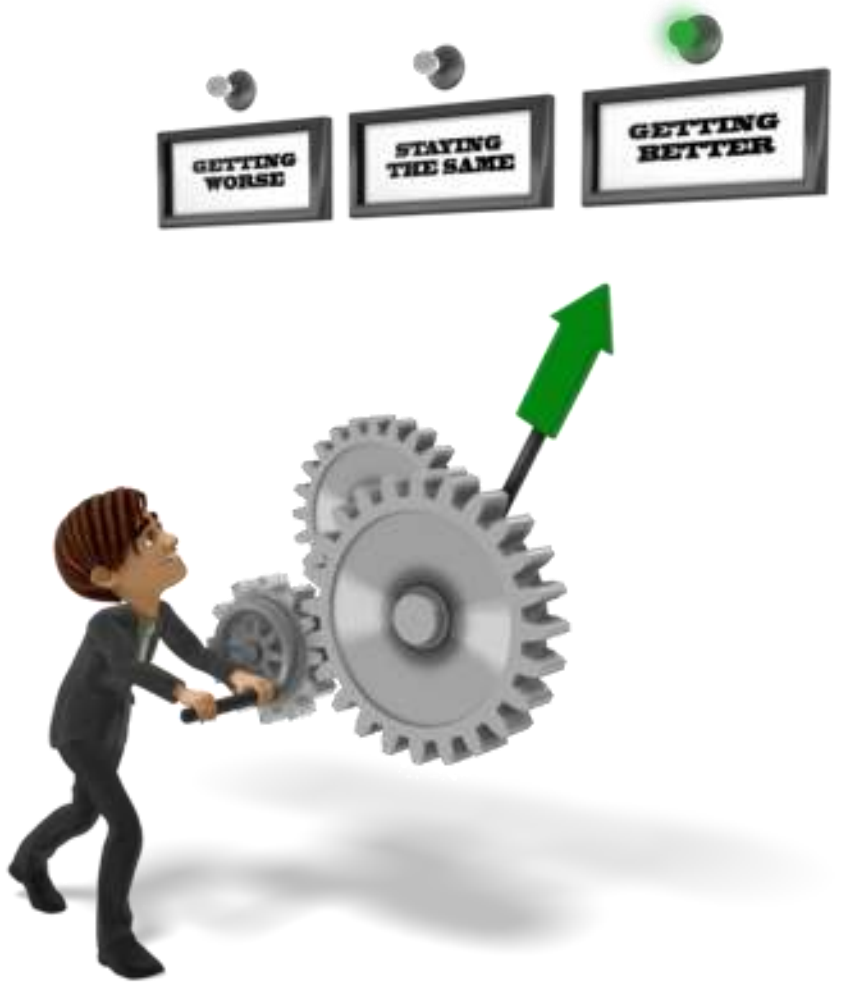
- **Design future state**
  - ✓ Improved process map with new workflow
  - ✓ Add controls, automation, and updated roles
  - ✓ Ensure goals align with business goals
- **Validate and test the new process**
  - ✓ Simulate or pilot with a small group
  - ✓ Collect feedback and update the new business process design
- **Implement and monitor**
  - ✓ Roll out the new process across the organization
  - ✓ Use key performance indicators (KPIs) - metrics to measure results
- **Continuous improvement**
  - ✓ Monitor KPIs and adjust accordingly to continue to improve over time

IOActive.

Beyond TARAs

What is this at a high level?

- Process improvement and optimization
- Can lead to
  - ✓ Reduction in costs and expenses
  - ✓ Improved turnaround time
  - ✓ Higher quality and greater consistency
- Not limited to TARA
- Program and process improvement can be applied anywhere
  - ✓ Cybersecurity
  - ✓ Information Technology (IT)
  - ✓ Operational technology (OT)
- How do we prioritize?

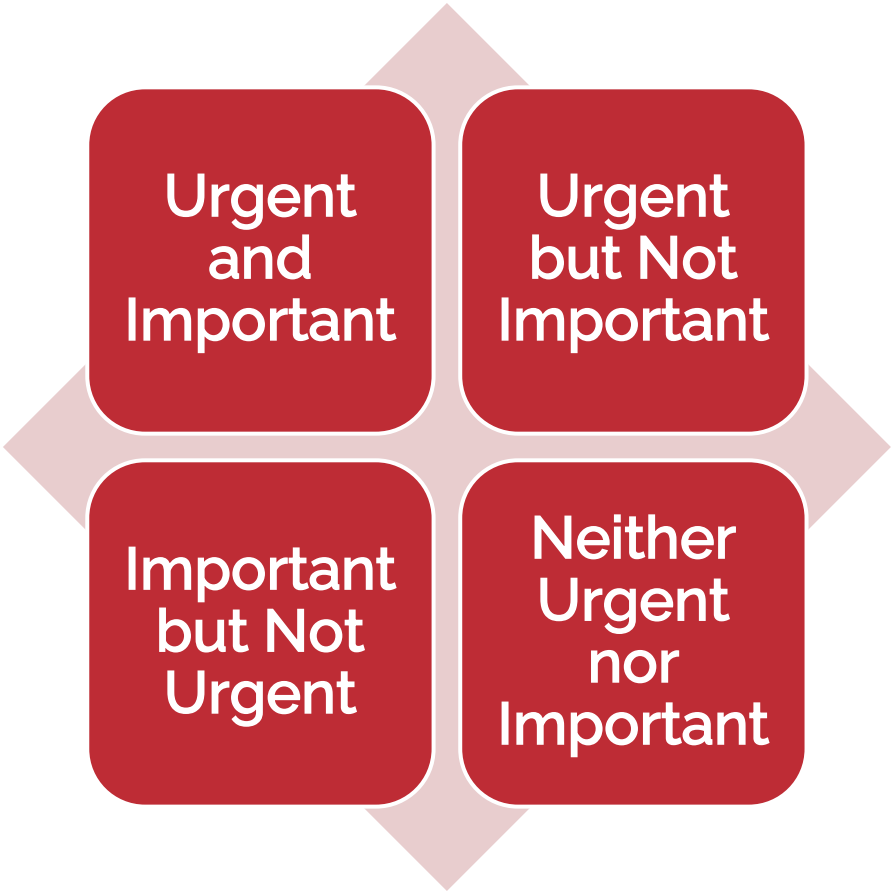


Prioritized Spending

Spending Prioritization

- Return on Spend (ROS): What are you paying?
- Return on Security Investment (ROSI): What value are you getting?
- Key questions:
  - How much is something costing you?
  - Are you getting a good return on your spend?
- Effective programs:
  - Align with governance expectations
  - Deliver measurable outcomes
  - Optimize resources and reduce waste

The Eisenhower Matrix



The Eisenhower Matrix

- **Urgent and Important:** Must-haves, like tools protecting your most targeted assets
- **Important but Not Urgent:** Strategic efforts, like employee training or improving logging infrastructure
- **Urgent but Not Important**: Fire-drill requests that burn budget but add little value
- **Neither Urgent nor Important:** Legacy tools collecting dust (and invoices)

Program Improvement and Optimization

Improve Program Efficacy

- Cost prioritization and process optimization are a powerful combination
- Streamlined processes reduce waste, rework, delays, and unnecessary spending
- Standardized methods and processes improve quality and consistency
- Prioritizes high value activities
- Helps measure what matters (KPIs)
- Maximize ROS/ROSI

Outside perspective

- Seasoned experts offer speed, experience, and objectivity
- Worked across multiple industries, seen common patterns and pitfalls
- Move faster than most internal teams alone
- Not replacing internal teams, but helping them become more effective
- Help accelerate ROI realization
- A little outside perspective might be just what your company needs to move forward with clarity and confidence

IOActive Approach

- Start with governance
- Review and evaluate operations
- Use real threat intelligence to drive priorities
- Industry-specific Tactics, Techniques, and Procedures (TTPs) yield real world specific areas and issues
- TTPs help steer resources towards likely high-impact areas
- **The goal:** faster, smarter, cheaper cybersecurity—without sacrificing protection.

Wrap-up

Wrap Up

- Framing the Challenge
  - Governance, ROI, and program efficacy
- TARAs as a Case Study
  - How Threat Analysis and Risk Assessment reveal strengths and weaknesses
- Survey Insights
  - Key findings from OEMs, suppliers, regulators, and fleets
- From Compliance to Value
  - Turning TARAs into safety-critical, value-driven processes
- Process Improvement
  - Lean, Six Sigma, and governance alignment
- Program Improvement and Optimization
  - Path forward to faster, smarter, cost-effective cybersecurity

IOActive.

Urban Jonson
urban.jonson@ioactive.com

Kevin Harnett
Transportation Cybersecurity Technical Advisor
kevin.harnett@ioactive.com
617-699-7086

John Sheehy
SVP, Research and Strategy
john.sheehy@ioactive.com

Services

- ✓ Security Program Efficacy
- ✓ Security Program Development & Management
- ✓ Virtual CISO
- ✓ Standards and Regulatory Gap Analysis
- ✓ Secure Development Lifecycle Support
- ✓ Threat Modeling