

AUTO-ISAC
AUTOMOTIVE CYBERSECURITY BEST PRACTICES

AWARENESS AND TRAINING

Best Practice Guide
Version 1.3

Traffic Light Protocol: WHITE.

This information may be shared in public forums.

Version History

This is a living document, which will be periodically updated under the direction of the Auto-ISAC Best Practices Working Group. We will track any updates in the table below.

Version Notes:

Version	Revision Date	Notes
v1.0	7 May 2018	
v1.1	30 November 2018	Changed from TLP Amber to TLP Green for release to industry stakeholders via request on Auto-ISAC website
v1.2	01 July 2019	Performed periodic continuity and consistency refresh across all Best Practice documents
v1.3	19 August 2019	Changed from TLP Green to TLP White for release to the public via request on Auto-ISAC website

Contents

Version History.....	i
1.0 Introduction	1
1.1 Best Practices Overview	1
1.2 Purpose.....	1
1.3 Scope	1
1.4 Audience	2
1.5 Authority and Guide Development	2
1.6 Governance and Maintenance	2
2.0 Best Practices	3
2.1 Framework for Awareness and Training in Vehicle Cybersecurity.....	3
2.2 Best Practices to Design Awareness and Training	4
2.2.1 Assessing Needs of the Business.....	4
2.2.2 Scoping Awareness and Training	5
2.2.3 Developing Strategy and Plan.....	6
2.3 Best Practices to Develop Awareness and Training	6
2.3.1 Developing or Acquiring Awareness Content and Products.....	7
2.3.2 Developing or Acquiring Training Curricula.....	8
2.3.3 Fostering Culture.....	9
2.4 Best Practices to Implement Awareness and Training.....	10
2.4.1 Communicating Strategy and Plan.....	10
2.4.2 Conducting Awareness Activities and Distributing Products	11
2.4.3 Conducting Training	11
2.5 Best Practices to Improve Awareness and Training	12
2.5.1 Monitoring and Reporting	13
2.5.2 Analyzing Effectiveness	14
2.5.3 Identifying Improvement Opportunities	15
Appendix A: Glossary of Terms	17
Appendix B: Additional References and Resources	18
Appendix C: Acronyms	19

1.0 Introduction

1.1 BEST PRACTICES OVERVIEW

This Best Practice Guide is one in a series of seven Guides intended to provide the automotive industry with guidance on the Key Cybersecurity Functions defined in the [Automotive Cybersecurity Best Practices Executive Summary](#):

1. Incident Response
2. Collaboration and Engagement with Appropriate Third Parties
3. Governance
4. Risk Assessment and Management

5. Awareness and Training

6. Threat Detection, Monitoring and Analysis
7. Security Development Lifecycle

Guides offer greater detail to complement the high-level Executive Summary. This Guide aligns with the “awareness and training” function and is made available for use by companies, as appropriate for their unique systems, processes, and risks.

1.2 PURPOSE

The purpose of this Guide is to assist automotive industry stakeholders with designing, developing, implementing, and improving vehicle cybersecurity awareness and training.

This Guide provides forward-looking guidance without being prescriptive or restrictive. These best practices are:

- **Not Required.** Companies have autonomy and can decide which of these practices to select and can adopt these practices based on their respective risk landscapes and organizational structures.
- **Aspirational.** These practices are forward-looking and voluntarily implemented over time, as appropriate.
- **Living.** Auto-ISAC plans to periodically update this Guide to adapt to the evolving automotive cybersecurity landscape.

1.3 SCOPE

This Guide describes key considerations for companies around vehicle cybersecurity awareness and training efforts. It contains best practices and implementation guidance for companies to design, develop, implement, and improve vehicle cybersecurity awareness and training, and integrate vehicle cybersecurity elements into existing cybersecurity awareness and training programs, as appropriate. These are voluntary, non-prescriptive, and aspirational practices.

The scope of the guide covers all phases of the vehicle lifecycle, including design, development, and post-production. These phases are described in Figure 1 below.

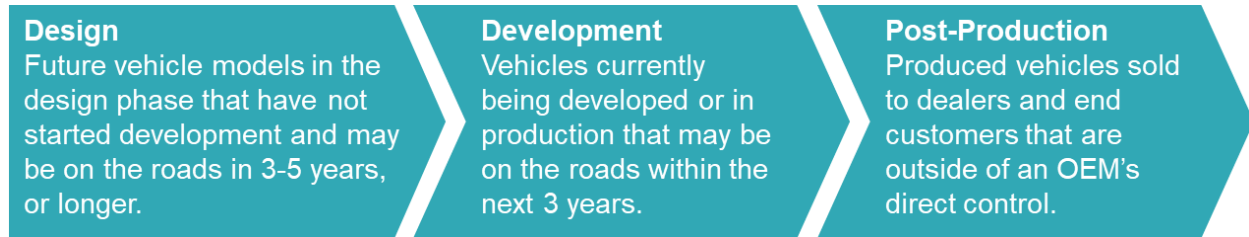


FIGURE 1: VEHICLE LIFECYCLE PHASES

1.4 AUDIENCE

This Guide was written for use by light-duty and heavy-duty vehicle OEMs, light-duty and heavy-duty vehicle suppliers, and commercial vehicle companies (e.g. fleets, carriers). It may also provide insights for other stakeholders across the connected vehicle ecosystem.

Within these organizations, this Guide is most relevant for vehicle cybersecurity managers, leaders, and senior executives responsible for vehicle cybersecurity awareness and training

1.5 AUTHORITY AND GUIDE DEVELOPMENT

The Auto-ISAC Best Practices Working Group wrote this Guide, with support from Booz Allen Hamilton vehicle cybersecurity SMEs who facilitated the Guide's development. The Working Group is comprised of over 130 representatives from Auto-ISAC Members, including:

AAA	FCA	Infineon	Mobis
Aptiv	Ford	Intel	Nissan
AT&T	General Motors	Kia	NXP
Auto Alliance	Global Automakers	Lear Corporation	Panasonic
Bosch	Geotab	Magna	Subaru
BMW	Harman	Mayer Brown	Toyota
Continental	Honda	Mazda	Volkswagen
Cummins	Honeywell	Mercedes-Benz	Volvo
DENSO	Hyundai	Mitsubishi Motors	ZF

The Working Group also coordinated with several external stakeholders and partners while developing this Guide, including NIST, NHTSA, and Aviation-ISAC.

Companies may implement these Best Practices while also referring to the References and Resources listed in Appendix B, which informed the development of these Best Practices.

1.6 GOVERNANCE AND MAINTENANCE

The Auto-ISAC Best Practices Standing Committee is responsible for the maintenance of the Guide, which will undergo periodic refresh to incorporate, as appropriate, lessons learned, new policies, updated or new engineering standards, and the like.

This Guide will be rolled out in phases and marked accordingly with the appropriate Traffic Light Protocol (TLP) classification:

- **First 3 months after publication: TLP Amber** - available exclusively to Auto-ISAC Members

- **3 to 9 months after publication: TLP Green** - released by request to industry stakeholders
- **9 months after publication: TLP White** - released to the public via the Auto-ISAC website (www.automotiveisac.com), subject to Board of Directors confirmation

2.0 Best Practices

This section identifies the primary elements of vehicle cybersecurity awareness and training activities and provides implementation guidance and considerations for each activity.

2.1 FRAMEWORK FOR AWARENESS AND TRAINING IN VEHICLE CYBERSECURITY

A cybersecurity awareness and training program is an organizational capability designed to improve the cybersecurity knowledge and mindfulness of employees and partners and reinforce positive cybersecurity practices.

The framework for vehicle cybersecurity awareness and training consists of four fundamental activities: Design, Develop, Implement, and Improve.

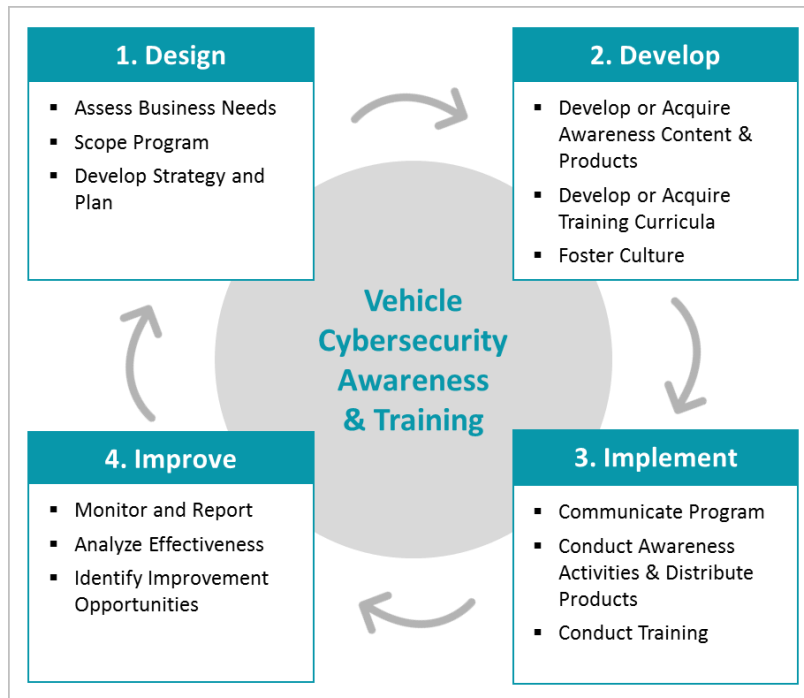


FIGURE 2: VEHICLE CYBERSECURITY AWARENESS AND TRAINING FRAMEWORK

These activities provide guidance and a framework that companies can use to design their own programs. To that end, this Guide does not prescribe specific requirements for awareness and training design, development, implementation, and improvement. Instead, it describes decision factors that companies can use to determine what is appropriate for their unique business environment and vehicle cybersecurity maturity.

2.2 BEST PRACTICES TO DESIGN AWARENESS AND TRAINING

Vehicle cybersecurity awareness and training design includes understanding the needs of the business, identifying the appropriate scope for the program, and defining an actionable strategy and plan.

2.2.1 Assessing Needs of the Business

Assessing an organization's vehicle cybersecurity awareness and training needs involves evaluating the current program coverage and identifying future goals and requirements.

There are many ways to understand the coverage of the current program. For example, current vehicle cybersecurity maturity, knowledge, and skill levels may be assessed by conducting a company-wide evaluation, whereas some departments may benefit from a more targeted approach. Possible evaluation methodologies include:

- Individual role-based knowledge assessments
- Focus group discussions
- Surveys and questionnaires
- Honest, open, direct-line management perspective communications
- On the job observations

Internal cybersecurity forums and events can be held to solicit direct feedback and concerns from managers, employees, and partners. Additionally, assessments of the current vehicle cybersecurity policies, frameworks, and awareness and training resources provided by the company can help create a comprehensive understanding of the current program coverage.

To evaluate the future goals and requirements of vehicle cybersecurity awareness and training, companies may consider a phased approach, which could involve:

1. Reviewing the organization's long-term product and technology roadmaps and plans to identify future needs of the business
2. Identifying the organization's cybersecurity goals
3. Translating the needs of the business and cybersecurity goals to future requirements for vehicle cybersecurity awareness and training

Awareness and training design and implementation best practices from industry peers and other infrastructure segments (e.g. financial services, aviation, telecommunication) are valuable resources when establishing vehicle cybersecurity awareness and training goals. It can also be helpful to review current measures of the effectiveness of the vehicle cybersecurity program to help ensure that the target goals are appropriate and aligned with projected threats and risks.

It is beneficial to engage a large group of internal and external stakeholders and SMEs to provide input for vehicle cybersecurity awareness and training design. Internal stakeholders typically include employees from departments such as Vehicle Cybersecurity, Human Resources, Training, Product Engineering, Research and Development, Manufacturing, Enterprise Cybersecurity, Information Technology, and Safety. External stakeholders may include cybersecurity and training partners, consultants, and service providers. Collaboration with stakeholders may help identify comprehensive, cross-functional needs of the business for vehicle cybersecurity awareness and training. Additionally, companies can partner with government agencies (e.g. NIST) to conduct an evaluation of cybersecurity maturity. The result of the needs

of the business assessment provides a basis for scoping vehicle cybersecurity awareness and training and developing a strategy and implementation plan.

2.2.2 Scoping Awareness and Training

Awareness efforts and training activities are different, and they complement each other to form a comprehensive awareness and training program. Awareness efforts encourage employees and partners to fully engage in training activities and training supports and enables the awareness program. In awareness activities, the learner is a passive recipient of information, whereas the learner in a training environment has a more active role.

Awareness efforts provide individuals with the resources to recognize cybersecurity concerns and respond accordingly. It is a continual process that explains what cybersecurity means to the organization and promotes positive cybersecurity behavior and culture. Awareness activities are typically brief and frequent in nature but may also scale with increasing needs for awareness as vehicle cybersecurity risks grow.

Training activities reinforce the awareness campaign by providing the knowledge and skills required to practice effective cybersecurity behavior. Training requires more concentration and time from employees and partners, and usually includes tests to measure comprehension of a finite set of knowledge. Training scope can vary from fundamental, portions of which can be used in an awareness campaign, to role-based topics, such as secure coding for embedded product engineers.

The target audiences for vehicle cybersecurity awareness and training may include, but is not limited to, employees and partners from the following departments:

- Executives
- Vehicle Cybersecurity
- Enterprise Cybersecurity
- Safety
- Research and Development
- Product Engineering
- Production Engineering
- Supply Chain / Procurement
- Information Technology
- Public Relations
- Customer Service
- Dealership and Repair Network

To define the knowledge and skill requirements of each target audience, companies should first understand the roles and responsibilities of the audience and then align vehicle cybersecurity awareness and training activities as appropriate.

It is important to integrate vehicle cybersecurity awareness and training into the vehicle development lifecycle. At the beginning of the development lifecycle, a vehicle cybersecurity “refresher” course held during the program kickoff can remind team members of their cybersecurity roles and responsibilities. On-demand modular training components help reinforce knowledge and skills required for each vehicle development lifecycle stage. Companies can also

evaluate existing development lifecycle training and combine vehicle cybersecurity activities into existing steps as appropriate.

When designing vehicle cybersecurity awareness and training activities, companies may choose to define a scope that is both reasonable and sustainable, while considering factors such as the time and budget required and availability of existing resources. As the potential impact of cybersecurity risks continues to grow, it is valuable to prioritize vehicle cybersecurity training and awareness. A well-trained workforce can help decrease the number and/or impact of cybersecurity incidents, which can help to retain customer confidence. It can be valuable to communicate these factors to senior leadership to establish buy-in and maintain prioritization of vehicle cybersecurity awareness and training.

2.2.3 Developing Strategy and Plan

Vehicle cybersecurity awareness and training support the overall business objectives around cybersecurity. It is important to identify the overarching learning objectives, which are impacted by factors such as the program scope, current maturity, organizational structure, and success measures. Companies may find it helpful to adopt the SMART (Specific, Measurable, Achievable, Relevant, Time-Bound) or comparable criteria when writing program objectives.

When developing an awareness strategy, companies may consider the following best practices:

- Following consistent messaging throughout all content
- Integrating awareness messaging with existing safety and enterprise cybersecurity awareness programs and products
- Focusing on changing behaviors through repetition
- Ensuring stakeholders' endorsement and support
- Soliciting end user ideas and encouraging feedback
- Measuring the effectiveness, success, and growth of the program

And when developing a training strategy, companies may consider the following best practices:

- Developing fundamental and role-based curricula
- Updating training to reflect changes to knowledge and skills requirements
- Updating content and delivery methods to reflect latest approaches and best practices
- Ensuring stakeholders' priority and support
- Reinforcing a culture of continuous learning
- Partnering with key departments
- Measuring the effectiveness, success, and growth of the program
- Inviting experts from enterprise cybersecurity and vehicle cybersecurity to exchange information
- Including specific training for employees and partners with cybersecurity responsibilities

While the implementation plans differ between awareness and training activities, it is important to consider elements such as timing, duration, delivery method, and assessment approach.

2.3 BEST PRACTICES TO DEVELOP AWARENESS AND TRAINING

With the vehicle cybersecurity awareness and training scope and strategy defined, the next step is to develop or acquire content. Awareness and training content should be flexible because

vehicle cybersecurity risks are constantly evolving as vehicle technologies advance and threat actors increase in sophistication.

Since vehicle cybersecurity shares many common practices with enterprise cybersecurity, it is often good practice to develop vehicle cybersecurity content in tandem with other cybersecurity training content, leveraging existing content where appropriate. However, there are distinct differences between the skills and knowledge needed for vehicle cybersecurity and those needed for enterprise cybersecurity, so it is also good practice to develop additional awareness and training content that is unique to each.

2.3.1 Developing or Acquiring Awareness Content and Products

Awareness efforts strive to build a consistent culture and maintain ongoing focus on cybersecurity across the broader organization. The content, which varies based on campaign or delivery medium, includes both company-wide and role-specific messaging. When evaluating awareness content and products, a company may consider its fundamental goals of awareness efforts which could include enabling some of the following behaviors:

- Integrating cybersecurity into all phases of product development
- Encouraging open, honest, and thorough communication between various organizational elements and incident response teams so that incidents can be addressed rapidly
- Identifying and reporting suspicious behavior as aligned with company policies
- Understanding that system features can be abused and that cybersecurity features can be bypassed
- Welcoming cybersecurity engineers into the product development teams

To encourage this behavior, it is helpful for relevant employees and partners to have a comprehensive understanding of vehicle cybersecurity. When developing or acquiring awareness content and products, it can be helpful to consider including the following topics, tailored for the organization where appropriate:

- Secure development lifecycle
- Vehicle attack vectors
- Legal and regulatory requirements
- Vehicle incident response process
- Similarities, differences, and relationships between cybersecurity, safety, and privacy
- Similarities, differences, and relationships between vehicle and enterprise cybersecurity
- Corporate cybersecurity operations
- Corporate governance
- Business risk

There are multiple internal and external resources that can provide source content and guidance on the identified topics, including:

- Internal:
 - Internal policies, procedures, and processes
 - Internal vehicle cybersecurity SMEs
 - Corporate and organizational cybersecurity processes
- External:

- Security conferences
- Regulatory requirements
- Information from Auto-ISAC partners
- Training providers
- Government publications
- Published standards (e.g. SAE/ISO, NIST)
- University and academia
- Other ISACs (e.g. Aviation-ISAC)

Companies may determine whether to create awareness content internally or acquire awareness content and products from external sources. There are potential pros and cons for each strategy.

	Pro	Con
Internally Developed Content	<ul style="list-style-type: none"> • Closer alignment with company-specific policies and procedures • Lower direct cost of production initially • More seamless integration into regular business flow 	<ul style="list-style-type: none"> • More time and effort from internal staff to keep content updated to industry standards • May miss key industry-wide topics • May require frequent maintenance to stay on the leading edge of industry practices
Externally Developed Content	<ul style="list-style-type: none"> • Provides new ideas • More comprehensive content • Faster time to implementation 	<ul style="list-style-type: none"> • May not be relevant to the company approach • May miss key organization-specific procedures • Higher direct cost of production • Requires review from internal training staff to ensure relevancy

Sometimes it is helpful to use a combination of the two approaches – developing a portion of the content internally, while acquiring another portion externally. For example, it may be more efficient to acquire foundational content (e.g. Internet of Things) from external sources and develop role-based content specific to vehicle cybersecurity internally.

2.3.2 Developing or Acquiring Training Curricula

Training drives the development and testing of applicable skills and knowledge through active engagements. There is a wide variety of training topics to consider when creating the training curricula. Vehicle cybersecurity training topics vary based on the needs of each company, but some topics to consider at a high level include:

- Vehicle risk analysis and assessment, including threat analysis
- Vehicle incident response
- Vehicle attacks and attack Proof-of-Concept (PoC)
- Secure lifecycle management
- Legal and regulatory requirements
- Customer requirements
- Security by design
- Privacy

- Governance
- Cryptography
- Secure coding
- Testing techniques (e.g. penetration testing, source code testing)

Training curricula and content may be developed internally or acquired from external sources; the potential pros and cons are similar to those of awareness content.

	Pro	Con
Internally Developed Content	<ul style="list-style-type: none"> • May be more relevant to the targeted audiences • Lower direct cost of production initially 	<ul style="list-style-type: none"> • Does not include an outside perspective • More time and effort from internal staff to keep content updated to industry standards
Externally Developed Content	<ul style="list-style-type: none"> • Faster time to implementation • Many external partners often provide a “train the trainer” option • Some training is beyond the technical expertise of internal staff and must be conducted by external experts 	<ul style="list-style-type: none"> • Less control over the content • Higher direct cost of production

Similar to awareness content, it may be beneficial to use a hybrid approach by integrating internally and externally developed material. A non-exhaustive list of available external resources can be found in Appendix B.

It is helpful to tailor training programs for audiences based on their needs and their specific roles. Companies may choose a portfolio of individual training courses that can be mixed and matched to provide a targeted set of training based on the needs of the audience. Best practices to consider when customizing training include:

- Matching knowledge and skill gaps to existing training resources
- Creating and testing a training course based on existing resources, and soliciting course feedback
- Hiring specialists to teach and/or develop content for subjects that are new or highly specialized
- Using local languages
- Embedding examples, stories, and business cases that the audience finds relatable
- Identifying the vehicle cybersecurity impact of specific roles
- Ensuring technical depth is appropriate for each role
- Identifying the involvement of each role in vehicle cybersecurity incidents
- Acquiring input from non-cybersecurity personnel

2.3.3 Fostering Culture

Vehicle cybersecurity culture should be reflected in the organization’s day-to-day activities, corporate processes, and vocabulary. An organization’s cybersecurity culture is vital to the organization’s long-term success. Setting reasonable vehicle cybersecurity expectations for employees and partners and identifying SMEs helps maintain culture throughout the organization.

It is beneficial to consider the following practices to build a strong vehicle cybersecurity culture:

- Discussing vehicle cybersecurity in relevant product design meetings
- Building in relevant cybersecurity deliverables throughout the product development process
- Emphasizing cybersecurity awareness at all vehicle-related functions of the company (e.g. purchasing, regulatory, engineering)
- Having a cybersecurity engineer or architect embedded part-time or full-time within the development teams
- Conducting a cybersecurity review at every phase of the vehicle development process

Measuring and reporting a company's cybersecurity culture is difficult as this is a qualitative measurement parameter. Information gathering techniques—such as on the job observations, surveys, or focus groups to track employee and partner behavior and alignment with the culture—may provide valuable qualitative evaluation results. However, there are some quantitative measures that can be used to monitor changes in cybersecurity culture, including:

- Number of cybersecurity conferences attended
- Number of cybersecurity presentations given
- Time spent with cybersecurity tutorials
- Trending of vulnerabilities and incidents

These measures are a way for leadership to gain visibility into the company's vehicle cybersecurity culture.

2.4 BEST PRACTICES TO IMPLEMENT AWARENESS AND TRAINING

Implementing vehicle cybersecurity awareness and training involves communicating the program to stakeholders, conducting the awareness activities, and conducting training.

2.4.1 Communicating Strategy and Plan

Senior leadership may consider emphasizing the importance of cybersecurity awareness and training to underscore its importance to the target audience. Suggested messaging includes the following topics:

- Cybersecurity is vital to company success
- Cybersecurity is an aspect of quality
- Cybersecurity affects the entire product lifecycle
- Cybersecurity takes a joint effort across departmental lines
- Cybersecurity requirements compliance helps safeguard customers and protect their privacy
- Cybersecurity training will be sustained and updated to maintain relevancy
- Cybersecurity training encompasses fundamental and role-specific curricula

The target audience for awareness and training plan communication include internal staff, suppliers, partners, and customers.

2.4.2 Conducting Awareness Activities and Distributing Products

The goal of a properly-designed awareness campaign is to set the conditions for consistent awareness of cybersecurity issues that results in desired behavioral changes, in line with company policy. Additionally, structured cybersecurity awareness campaigns allow for more targeted distribution of specific messages that may be in response to an incident or emerging threat.

There is a wide variety of awareness content distribution methods. The success of each method depends on variables such as an organization's cybersecurity culture, operating model, cybersecurity maturity, and the level of complexity of the awareness content. Awareness content can be categorized into three main types: physical, digital, and activity.

Type	Example	Pros	Cons
Physical	<ul style="list-style-type: none"> • Pamphlet • Poster • Mail • Electronic signage/ display monitors 	<ul style="list-style-type: none"> • Lower budget • Lower implementation effort • Larger audience 	<ul style="list-style-type: none"> • Limited audience engagement • Difficult to measure effectiveness
Digital	<ul style="list-style-type: none"> • Email • Webpage (e.g. Wiki) • Electronic document • Secure portals and incident response websites 	<ul style="list-style-type: none"> • Lower budget • Faster delivery • Larger audience 	<ul style="list-style-type: none"> • Limited audience engagement • Difficult to measure effectiveness • Special system requirements
Activity	<ul style="list-style-type: none"> • Seminar • Exercises • Cyber contest 	<ul style="list-style-type: none"> • Stronger audience engagement • Ability to measure effectiveness 	<ul style="list-style-type: none"> • Higher cost • Limited scale • Participation time requirements

When determining the best delivery method for certain awareness content, consider the following factors:

- Time required by the intended audience
- Maintaining the audience's focus and interest
- Level of technical complexity of the content
- Audience's preexisting knowledge of the content
- Requirements for knowledge to be shared
- File size of the content and bandwidth available to staff for downloads and content streaming
- Content relevance for the intended audience

2.4.3 Conducting Training

Similar to awareness efforts, training activities can be conducted through a variety of channels. The following table provides a comparison of the different types of training.

Type	Pros	Cons
Webinars, Online Videos	<ul style="list-style-type: none"> • Larger audience 	<ul style="list-style-type: none"> • Difficult to maintain audience's attention

Type	Pros	Cons
	<ul style="list-style-type: none"> Available for repeated viewing (Recorded) Flexible scheduling 	<ul style="list-style-type: none"> Limited measuring of audience's understanding
Conferences	<ul style="list-style-type: none"> Captive audience Uninterrupted training Promotes discussion of alternate perspectives 	<ul style="list-style-type: none"> Costly Difficult to tailor content for all audiences Logistical challenges
Internal Seminars, Classroom Training	<ul style="list-style-type: none"> Content tailored to corporate objectives Promotes internal discussion Allows for gathering feedback 	<ul style="list-style-type: none"> Somewhat costly Limited outside perspective Fixed scheduled Required time commitment
Computer-Based Training	<ul style="list-style-type: none"> Larger audience Allows for testing Allows for tracking of compliance 	<ul style="list-style-type: none"> Somewhat costly

Vehicle cybersecurity awareness and training can be built into existing on-boarding procedures to help ensure new employees understand the company's vehicle cybersecurity culture, processes, and procedures from day one. However, it is also an ongoing process that occurs throughout an employee's career. Determining the most effective delivery method depends on factors such as time commitment, level of detail, level of engagement, program guidelines, and learning style.

Additionally, the depth and/or breadth of the training curricula is highly dependent on the company's needs and the audience roles and responsibilities. This will impact the distribution of resources dedicated to the training program. These variables are important considerations to ensure training needs are being met across the organization.

When conducting training, it is important to consider that individuals have different learning styles. To help ensure the vehicle cybersecurity awareness and training is effective across the organization, it can be beneficial to have a variety of implementation methods. For example, consider including more advanced training delivery methods and approaches such as simulations, audio-visual interaction, and kinesthetic elements. This may make the training more accessible and more effective as the audience can engage with the content.

Training effectiveness can be measured through post-training tests, technical competency evaluations, and on-job observations. To drive training compliance, awareness and training program administrators may consider tracking training completion and coordinate with human resources or line managers to take follow up action if needed. Leadership may want to consider a compliance strategy that focuses on positive reinforcement. Instead of demanding training be completed, managers can communicate that participants may qualify for a reward.

2.5 BEST PRACTICES TO IMPROVE AWARENESS AND TRAINING

Vehicle cybersecurity awareness and training may evolve with needs of the business and the vehicle risk landscape. Monitoring and improvement efforts help to maintain a skilled and knowledgeable workforce.

2.5.1 Monitoring and Reporting

It is important to track vehicle cybersecurity awareness and training results and report appropriate metrics to the leadership. When monitoring vehicle cybersecurity awareness and training, consider elements that include, but are not limited to, the following:

Monitoring Area	Key Questions
Accessibility of the content	<ul style="list-style-type: none"> • How often are trainings offered? • How is the content delivered? • Is the training on-demand?
Quality of the content	<ul style="list-style-type: none"> • Is the content clearly presented? • Is the content accurate? • Is the content up-to-date? • Are participants satisfied with the quality of the content?
Relevancy of the content to each participant	<ul style="list-style-type: none"> • Does the content align with the audience's roles and responsibilities?
Comprehension of the information	<ul style="list-style-type: none"> • Do participants understand the information? • How are participants performing on quizzes and tests during training? • Does the instructor present knowledge in an effective and understandable manner?
Retention of the knowledge	<ul style="list-style-type: none"> • Are the skills and knowledge being used appropriately?
Alignment of the program to goals/objectives	<ul style="list-style-type: none"> • Does the awareness campaigns and training content align with the program scope?
Alignment with the intended vehicle ecosystem elements	<ul style="list-style-type: none"> • Does the content sufficiently cover the intended vehicle ecosystem?
Alignment with the changing landscape	<ul style="list-style-type: none"> • Does the awareness campaigns and training content address changing cybersecurity vulnerabilities, technologies, and threats?
Participation in the program	<ul style="list-style-type: none"> • What percentage of the target audience has completed training? • What percentage of the target audience is exposed to awareness content? • Is participation being tracked and managed?

The above questions can be customized based on a company's strategy and maturity. These answers provide both qualitative and quantitative information to monitor vehicle cybersecurity awareness and training effectiveness and compliance. To maintain a skilled and knowledgeable workforce, both effectiveness and compliance are necessary. Additionally, this information can be compared to the program scope to determine whether the program meets the organization's vehicle cybersecurity needs and objectives.

In addition to information gathered when monitoring effectiveness and compliance, other internal and external resources can be used to monitor the program, including:

- Internal:
 - Periodic surveys of participants to identify strengths and weaknesses
 - Evaluation of cybersecurity defects in product lifecycle
 - Human resources feedback from performance planning reviews
 - Tabletop exercises
 - Architecture and system analysis
 - Internal audits of compliance to internal cyber policies and processes
 - Vehicle cybersecurity incident response performance
- External:
 - Analysis of program effectiveness by external vendor
 - Shared learning with other industry representatives
 - Best practices identified by government agencies (e.g. NHTSA, NIST)

There are also opportunities to integrate the vehicle cybersecurity awareness and training evaluation into supplier relationships. Leadership may consider including an analysis of partners' awareness and training maturities to evaluate the impact on products and internal processes.

Monitoring has elements of both top-down and bottom-up processes because there are company-wide and role-specific awareness and training content. At the corporate level, senior leaders may evaluate overall program performance to identify any adjustments needed to the overarching strategy. Bottom-up monitoring may occur at business units or by cybersecurity teams to monitor role-specific effectiveness and compliance and give leadership visibility into role-specific performance.

Program metrics should be reported to key stakeholders who can adjust the program. Typically, this includes leaders in Vehicle Cybersecurity, Human Resources, Legal, Risk Management, and Product Development.

2.5.2 Analyzing Effectiveness

At a high level, vehicle cybersecurity awareness and training can be considered effective if specific measures show increasing or acceptable institutionalization of vehicle cybersecurity fundamentals and practices in line with established goals and objectives. This requires information to be compared to baseline metrics or previously defined effectiveness. Metrics to determine effectiveness may include:

- Average Time to Respond (ATTR) between incident and response
- Correlation of product vulnerabilities to training compliance
- Level of training needed for target audiences
- Allocation of time and resources to training
- Availability of training content (e.g. not available, under development, initial release)
- Percentage of target audience that received or completed training
- Percentage of target audience that successfully passed tests on content (e.g. 80% on tests)
- Annual survey results of target audiences
- Compliance with standards, requirements, and regulations

It can also be useful to analyze effectiveness based on the trends of certain types of vulnerabilities if relevant to current designs. However, such analysis should consider that improving culture, skills, and knowledge may increase reported cybersecurity events. As employees and partners become more aware of cybersecurity in their daily work, opportunities to invoke an incident response plan may become more recognizable.

Assessment of overall vehicle cybersecurity program maturity and benchmarks can help measure progress against the company's established awareness and training objectives. Establishing precise quantitative measures of effectiveness is difficult because the awareness and training content may have identified threats that were not anticipated or more difficult to resolve. Therefore, companies may choose to consider industry best practices to establish baseline competencies and performance measures. To measure program effectiveness, consider evaluating the following areas:

- **Security by design:** Is cybersecurity effectively included in design processes?
- **Risk assessment and management:** Are risk treatments performed for identified risks?
- **Threat detection and protection:** Are threats detected appropriately? Is protection in place for identified threats?
- **Incident response:** Are cybersecurity incidents identified and resolved effectively?
- **Cybersecurity testing:** Are results from targeted cybersecurity testing and vulnerability disclosure improving?

As employees and partners become more skilled and the business evolves, it is important for companies to maintain ongoing assessments of the evolving needs of the business and update vehicle cybersecurity awareness and training as needed.

Annual program evaluation helps maintain continued relevancy, effectiveness, and alignment with overarching vehicle cybersecurity awareness and training goals and objectives. Existing training should be regularly evaluated against emerging threats, vulnerabilities, and technologies, though changes may occur less frequently. New training may also target the acquisition of new products or processes as they impact the development lifecycle.

2.5.3 Identifying Improvement Opportunities

Opportunities for improvement can be triggered by internal changes (e.g. cybersecurity maturity, organizational structuring, staff hiring) and by external changes (e.g. technology evolution, industry best practices development, changing threat landscape, new legislation). To identify opportunities to improve vehicle cybersecurity awareness and training, consider:

- **Internal:**
 - Feedback from participants of the program
 - Results from audits on employee and partner knowledge and skill
 - Correlation between cybersecurity testing results and training capabilities
 - Correlation between identified vulnerabilities and training topics
 - Correlation between number of identified incidents and training topics
 - Guidance from internal cybersecurity specialists
- **External:**
 - Current trends, technologies, threats, and research

Traffic Light Protocol: White (May be shared in public forums)

- Information from conferences regarding industry changes and changes in training methodologies
- Security standards, regulations, and legislation
- Performance and processes of industry partners
- Guidance from external cybersecurity specialists

Vehicle cybersecurity awareness and training should be re-designed as often as needed. If the program is not meeting the needs of the business, it is time to recalibrate. All the effectiveness measures presented in Sections 2.5.1 to 2.5.3 are factors in determining if the program requires updating or re-design. Additionally, companies may regularly consider whether the vehicle cybersecurity awareness and training objectives, scope, strategy, and plan need to be revised to reflect the changing needs of the business. It helps to implement feedback collection processes to regularly gather inputs from cross-functional employees and partners on potential improvement opportunities for vehicle cybersecurity awareness and training.

Appendix A: Glossary of Terms

Relevant terms used in this Guide are defined below.

TERM	DEFINITION
Awareness	Efforts intended to enable individuals to recognize cybersecurity concerns and respond accordingly.
Awareness and Training Program	Organizational capability designed to improve the cybersecurity knowledge and mindfulness of employees and partners and reinforce positive cybersecurity practices.
Culture	The set of shared attitudes, values, goals, and practices that characterizes an institution or organization.
Partner	Contractor, vendor, supplier, or other third-party personnel.
Penetration Testing	The practice of testing a system, network or application to find vulnerabilities that a threat actor could exploit.
Training	Activities that strive to produce relevant and needed cybersecurity skills and competencies.
Vehicle Cybersecurity	The activities, processes, and capabilities that protect, detect and respond to cyber occurrences (e.g. remote control, unauthorized access, disruption, manipulation) that actually or potentially result in adverse consequences to a vehicle, connected infrastructure, or information that the vehicle processes, stores, or transmits.

Appendix B: Additional References and Resources

The following References and Resources provide additional content and expertise for companies to consider in conjunction with the Best Practices discussed in this Guide.

REFERENCES – DOCUMENTS THAT MAY OFFER ADDITIONAL IMPLEMENTATION GUIDANCE
Association of Corporate Counsel State of Cybersecurity Report < link >
Department of Defense Cyber Strategy < link >
ISO/IEC 27000 Information Security Management Systems < link >
NIST SP 800-181 NICE Cybersecurity Workforce Framework < link >
NIST SP 800-50 Building an Information Technology Security Awareness and Training Program < link >
Society of Human Resource Management Training Design, Development, and Implementation Instructor's Manual < link >
RESOURCES – ORGANIZATIONS THAT MAY OFFER ADDITIONAL TRAINING RESOURCES
Automotive Information Sharing and Analysis Center (Auto-ISAC) < link >
Coursera < link >
Cybersecurity and Information Systems Information Analysis Center < link >
Cybersecurity Nexus ISACA CSX < link >
Defense Information Systems Agency Cybersecurity Education < link >
Department of Homeland Security Cybersecurity < link >
Escrypt < link >
Microsoft "Trustworthy Computing" < link >
Multi-State Information Sharing and Analysis Center < link >
MIT Continuing Education < link >
MIT OpenCourseWare < link >
National Credit Union Administration < link >
Office of Personnel Management Training and Development < link >
Riscure < link >
SAE Learning < link >
SANS Institute < link >
YouTube < link >

Appendix C: Acronyms

ATTR	Average Time to Respond
Auto-ISAC	Automotive Information Sharing and Analysis Center
ISAC	Information Sharing and Analysis Center
ISO	International Standards Organization
MIT	Massachusetts Institute of Technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
POC	Proof of Concept
SAE	Society of Automotive Engineers
SANS	System Administration, Networking, and Security Institute
SME	Subject Matter Expert
SMART	Specific, Measurable, Achievable, Relevant, Time-Bound
TLP	Traffic Light Protocol