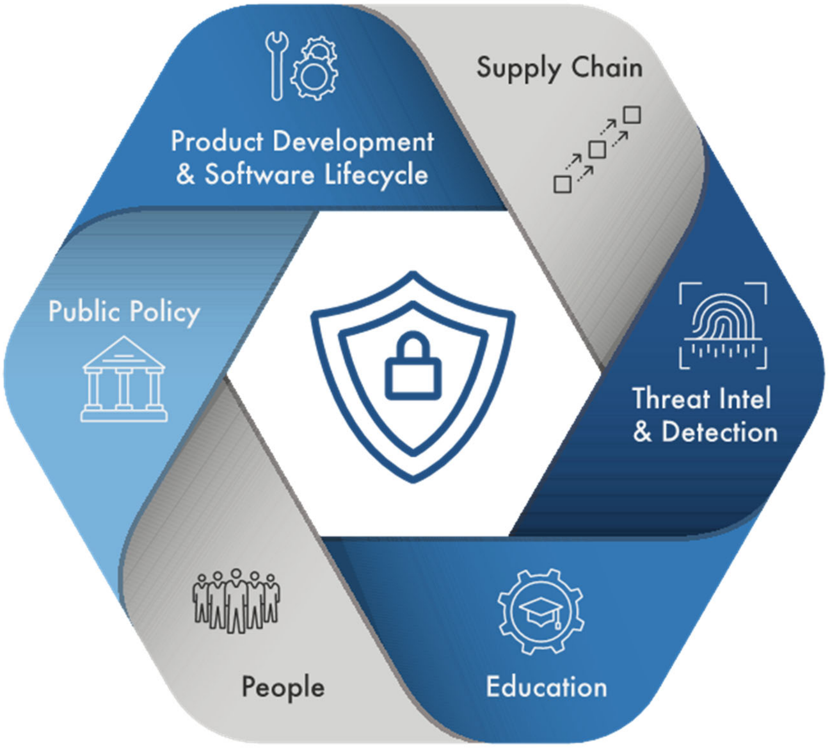
IDENTIFYING RISKS OF ADVANCED VEHICLE TECHNOLOGIES

Automotive Cybersecurity: More Than Technical Risks



*Chris Bonnette, Jason Carnes, Tim Leaf, Hannah Lensing, Kristie Pfosi,
David Sasaki, Jeff Stewart, and Lisa VanSlyke*

DHS Public-Private Analytic Exchange Program 2019

Table of Contents

Executive Summary

Advanced vehicle technologies, which encompass increasing degrees of vehicle automation and connectivity, have created the possibility of a catastrophic impact from the exploitation of automotive cybersecurity vulnerabilities. Thus, a closer look at the potential risks associated with advanced vehicle technologies is needed to inform risk management approaches in both the private and public sectors with regard to the threats, vulnerabilities, and potential consequences of exploitation of vehicle cybersecurity vulnerabilities. It is important to understand how different parts of the complex automotive ecosystem conceptualize cybersecurity risks, and the factors governing the presentation and management of these risks.

Our research identified six categories of risk, or risk areas, shown below. As categories, none of these are unique to the automotive industry. However, within each category, the nature of the automotive industry, its technologies, and its operating environment do provide unique challenges that manifest as cybersecurity risks to vehicles and particular to the automotive sector. Our key findings in each of these areas are:

1. **Product & Software Development.** Building a product with security in mind must begin in the earliest stage of product development. Historically, security risk assessment was not fundamentally built into automotive product and software development; organizations are now starting to prioritize these activities. Recent movement toward adopting a Secure Development Lifecycle approach promises significant improvements in vehicle cybersecurity, yet the process of this transition also poses its own forms of risks.
2. **Supply Chain.** The supply chains for advanced automobiles will continue to become increasingly complex. Furthermore, automotive OEMs will experience decreased control over the components and software implemented into their vehicles. These issues create risks to/from advanced vehicle technologies that must be addressed by a comprehensive and coordinated approach to end-to-end cybersecurity across the automotive supply chain.
3. **Threat Intelligence & Detection.** Cyber intelligence, threat analysis, and early detection are critical to risk management of product cybersecurity in the automotive industry. However, detection measures are only of value if proper response mechanisms are in place. Parallel maturation of automotive cyber intelligence, threat analysis and detection, and incident response is crucial to determining and addressing risks.
4. **People.** People are what enable continuous innovation and advancement of vehicle technology. They can also be the source of the greatest risks to vehicle cybersecurity. Appropriate leadership, organizational culture, and personnel security practices are crucial to mitigating risks associated with people in the automotive sector.
5. **Education.** Cybersecurity awareness and training programs enable advanced vehicle technologies and must go beyond the traditional educational model. The success of these efforts benefit from executive support and information sharing outside the organization.
6. **Public Policy.** Public policies, while often expected to provide improved cybersecurity measures, can actually create new risk areas which the automotive industry will be limited in mitigating.

We hope this work will provide some illumination on the scope and nature of the risks associated with advanced vehicle technologies.

“Special thanks to the silent professionals and the companies, which contributed to this product, who make countless impacts and work tirelessly to keep one step ahead of our adversaries”

Introduction

Advanced vehicle technologies, which encompass increasing degrees of vehicle automation and connectivity, have created the possibility of a catastrophic impact from the exploitation of automotive cybersecurity vulnerabilities. Over the last decade, public reporting has attributed real-world, kinetic effects from cyber operations, even on 'air-gapped' cyber-physical systems.[1] Academia first made vehicle cybersecurity risks public in 2010.[2] In the years that followed, the security community identified some inherent weaknesses in modern vehicle architectures. Charlie Miller and Chris Valasek made national headlines in 2015 when they demonstrated to Andy Greenberg, a technology journalist, the effects of exploiting vulnerabilities in certain connected vehicle technologies.[3] This in turn spurred the recall of 1.4 million vehicles, a class action lawsuit (still in litigation), and proposed legislation.[4] Industry and government both acknowledged the potential for devastating consequences if a threat intends to cause harm and began to more vigorously approach vehicle cybersecurity. However, serious potential risks to and from advanced vehicle technologies remain. For example, earlier this year researchers at Georgia Tech concluded that "just 13 compromised vehicles/km/lane on the Manhattan street network is enough to cause citywide disruption, wherein portions of the city become disconnected from key services."[5]

Thus, a closer look at these potential risks is needed to inform risk management approaches in both the private and public sectors with regard to the threats, vulnerabilities, and potential consequences of exploitation of vehicle cybersecurity vulnerabilities. It is important to understand how different parts of the complex automotive ecosystem conceptualize cybersecurity risks, and the factors governing the presentation and management of these risks. While we have categorized the risks we have identified, clearly, many of these risks are intricately and inherently interrelated to one another.

The scope of our analysis focuses on connected and at least partially automated, road-legal highway vehicles, both light-duty and heavy-duty (i.e. cars and commercial trucks). The primary audience for this work product includes senior leaders in both private sector firms and relevant public sector agencies, in addition to mid-level intelligence analysts and industry professionals.

[1] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired, July 11, 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

[2] Karl Koscher, et al. "Experimental security analysis of a modern automobile." 2010 IEEE Symposium on Security and Privacy, IEEE, 2010.

[3] Andy Greenberg, "Hackers Remotely Kill A Jeep On the Highway — With Me In It," Wired, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[4] Andy Greenberg, "Chrysler and Harman Hit With A Class Action Complaint After Jeep Hack," August 4, 2015, https://www.wired.com/2015/08/chrysler-harman-hit-class-action-complaint-jeep-hack/.

[5] Skanda Vivek, David Yanni, and Peter J. Yunker, "Cyber-physical risks of hacked Internet-connected vehicles," Physical Review E, Volume 100 Issue 1, published July 30, 2019, p. 6,

Methodology

This AEP team developed the information in this report through its independent research efforts over the course of the eight months of the project period. For part of this research, the team engaged in private discussions and interviews with a range of stakeholders. These included elements of the U.S. Department of Transportation and the U.S. military, state law enforcement agencies, automotive OEMs, Tier 1 suppliers, and industry associations. The team also conducted additional open source research and literature reviews.

The views, opinions, and/or findings contained in this report are the product of the combined efforts of the individuals on this AEP team, and should not be construed to represent the views, opinions, or positions of their respective employers or any other affiliated entities. Where possible, citations to publicly available sources are provided throughout this document. Otherwise, the information presented represents the synthesis of this team's research discussions and internal analyses of the information identified through its research.

Organization of Report

Our report presents six categories of risks associated with advanced vehicle technologies. These are:

1. The vehicle **product development and software lifecycle;**
2. The **supply chain** supporting vehicle production and operation;
3. The **people** involved in advanced vehicles, both their production and use;
4. **Education** of the workforce producing and consumers using advanced vehicles;
5. **Cyber Threat Intelligence and Threat Detection** pertinent to advanced vehicles;
6. **Public Policy** impacting advanced vehicles.

In each of these categories, we have researched and assessed the factors affecting or creating risks in these categories. We then delineate selected specific risks or risk areas associated with advanced vehicle technologies. Finally, we also present some considerations for mitigating the resultant risks.

Product & Software Development

Building a product with security in mind must begin in the earliest stage of product development. Historically, security risk assessment was not fundamentally built into automotive product and software development; organizations are now starting to prioritize these activities. Recent movement toward adopting a Secure Development Lifecycle approach promises significant improvements in vehicle cybersecurity, yet the process of this transition also poses its own forms of risks.

Product & Software Development Overview

Traditional automotive product development and software lifecycles have not typically or adequately incorporated cybersecurity concerns. For decades there was little need to, since vehicles were largely isolated machines and predominantly mechanical. However, as modern vehicles become increasingly connected and automated, the need to assess cybersecurity risks inherent in product development—and to develop cybersecurity protections during product development—increases as well. External communication technologies like cellular, WiFi, Bluetooth, and key fobs can provide remote access to the vehicle. And, as security researchers have demonstrated, these connections can be used to gain control of computerized critical vehicle functionality such as steering, braking, and throttle control.[6] The confluence of these technological changes presents risks associated with traditional automotive product and software development processes and lifecycles.

Additionally, in comparison to some other segments of the Internet of Things, the automotive industry has certain constraints that impact the ability to add traditional cybersecurity technologies and approaches, such as the factors discussed below.

One approach many automotive companies are taking to mitigate the risks associated with their product development processes is to move to a Secure Development Lifecycle (SDL) process. The transition to an SDL model from traditional practices carries its own risks as well.

Factors Shaping Automotive Product and Software Development Lifecycle Risks

Several attributes of the automotive design, development, and manufacturing requirements and processes act as factors creating or exacerbating cybersecurity risks associated with product and

[6] Chris Valasek and Charlie Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," White Paper, August 10, 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf.

software development. These include:

Safety-critical systems Driver occupant and road user safety are paramount in the vehicle design.

Extended development cycle The average vehicle development timeline is approximately four years from concept to production. This means the automotive designs must be dynamic during product development to keep pace with newly discovered cyber vulnerabilities.

Lengthy consumer usage lifecycle Average ownership period for a passenger vehicle is ten or more years. For commercial vehicles, this can be much longer. Relative to most other consumer electronic devices, especially those with direct risk to human life, security maintenance over this long period poses heightened product lifecycle challenges.

Highly complex systems Modern vehicles have over 100 unique Electronic Control Units (ECUs), each with a combination of hardware, software, and firmware, totaling over 100 million lines of code.

Highly constrained design parameters There are strict reliability, real-time, and availability requirements (e.g., fast boot times, low latency, etc.) for automotive systems for occupant safety and user experience. Lean design principles and cost sensitivities drive minimized microprocessor computing power, data storage, and network bandwidth to accommodate cybersecurity countermeasures.

Post-production support Under the current vehicle ownership model (predominantly individual private owners), it is at the owner's discretion to download software security patches and/or to perform regular maintenance in a timely manner to address known vulnerabilities. The population of vehicle owners is both diverse and not defined or constrained by the OEMs. Furthermore, "right to repair" agreements and legislation grant full read/write privileges to modify vehicle software to all users, independent of malicious intent (see Public Policy section, p. 21).

Complex supply chain Vehicle architecture must integrate those 100+ ECUs and component modules provided by a diverse set of suppliers into a reliable, high-performance system. Each ECU or component supplier in turn relies on a sub-tier of component suppliers using a combination of proprietary and open source software, in a globalized development environment spanning all times zones and many languages.

Product & Software Development Lifecycle Risks

Risk Area: Organizational Culture

Our research indicates that the culture of an automotive sector firm can make or break its ability to assess and mitigate cybersecurity risks of the product development process. Some industry interviewees are relatively advanced in their security culture development, while others are still in the beginning phases. For those more mature organizations, it was clear that the security culture was embedded from the top down.

Cybersecurity is not a "bolt on" solution that can be added to existing products to make them cyber secure. Rather, security is integral to the product itself, and needs to be woven into the product architecture and development. The organizational culture permeates the product development process. A successful cybersecurity culture is inculcated similarly to safety and quality, in that it is "everyone's responsibility." It is inherent in each and every hardware and software product developed by the company and blended into the corporate culture. Failures to appropriately evolve the organizational culture create greater risks to vehicle cybersecurity.

Recommendation: *The automotive SDL ensures that appropriate cybersecurity protections are identified in the early stages of design, e.g. during vehicle electrical architecture planning, when implementation costs are lower and there is time to consider design interactions that might affect cybersecurity. The SDL must be considered by all OEMs and suppliers, as it may affect the design and development of all vehicles and vehicle components, both hardware and software.*

Risk Area: Budget and Schedule Constraints

While tech industries are looking to be lean, agile, and fast-to-market in order to drive revenue and minimize costs, incorporating cybersecurity into product design and development takes both time and money. This is no different in the automotive industry, yet the consequences can be higher than in other tech industries. Failures to budget and schedule automotive product development processes with this in mind heighten vehicle cybersecurity risks.

Traditionally, the automotive business case has not factored in the added cost, resources, and schedule accommodations for cybersecurity risk analysis and development of countermeasures based on the feature set being offered. Cybersecurity has largely been perceived as an area for cost avoidance. Without explicit consumer demand or specific vehicle cybersecurity regulatory requirements, as development budgets are scrutinized or constrained, cybersecurity development competes against added advancement of technological features. Thus, it is commonly cut from lean programs.

Recommendation: Cybersecurity teams, tools and resources do not come for free, and they need to be included either as a direct or overhead cost (depending on organizational and costing structures) in the product development budget.

Risk Area: Transition to a Secure Development Lifecycle Approach

The automotive SDL ensures that appropriate cybersecurity protections are identified in the early stages of design, e.g. during vehicle electrical architecture planning, when implementation costs are lower and there is time to consider design interactions that might affect cybersecurity. The SDL can be an effective mitigation of the risks identified above, and must be considered by all OEMs and suppliers, as it may affect the design and development of all vehicles and vehicle components, both hardware and software.

However, implementing a strong security posture and transitioning to an SDL for all products does not happen quickly or easily. There are significant changes required within the organization to educate the workforce on new processes and techniques. As with any significant organizational change, there is a risk of a temporary decrease in performance or effectiveness during a transitional period, as teams acclimate to new processes and gain the requisite experience. This translates to potential risk to vehicles in the design and development pipeline during such a transitional period.

Recommendation: *Successful integration of the automotive SDL includes cybersecurity technical experts in all phases of the development process, from initial conception, architecting, through to production launch. Added cybersecurity design reviews, code reviews, and on-going testing is overlaid and integrated into the product development lifecycle to resolve cybersecurity risks early in the development cycle to minimize cost and timing impact. Leadership commitment is required to ensure this process change is fully absorbed into the organization.*

Supply Chain

The supply chains for advanced automobiles will continue to become increasingly complex. Furthermore, automotive OEMs will experience decreased control over the components and software implemented into their vehicles. These issues create risks to advanced vehicle technologies that must be addressed by a comprehensive and coordinated approach to end-to-end cybersecurity across the automotive supply chain.

Automotive Supply Chain Overview

The automotive supply chain is highly complex, with vehicles containing over 20,000 parts from diverse suppliers across the globe.[7] As automotive companies continue to develop increasingly connected and advanced vehicles, their supply chains will continue to transform as well. Automobile manufacturers will continue to diversify their supply chains to include more digital component and software suppliers. These new suppliers provide both automotive parts and systems to support vehicle functions, automation, and connectivity. Additionally, automotive OEMs are entering into service agreements with wireless, telematics, software, and cloud service providers that do not necessarily conform to the traditional tiered supply chain model.

Factors Affecting Automotive Supply Chain Risks

In any supply chain, cybersecurity is not just an IT or technology problem, it is a people, processes, and knowledge problem.[8] In looking at the supply chain broadly, we have identified three primary factors affecting risk in the advanced vehicle supply chain: evaluating the people, processes, and common knowledge of automotive supply chains. These factors contributing to risk in vehicle supply chains are highlighted below:

[7] Shefali Kapadia, "Moving parts: How the automotive industry is transforming." (website), February 20, 2018, https://www.supplychaindive.com/news/moving-parts-how-the-automotive-industry-is-transforming/516459/.

[8] National Institute of Standards and Technology, "Best Practices in Cyber Supply Chain Risk Management," (conference materials), https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

Component and Software Security Testing Limitations

OEMs and Tier-1 suppliers use a risk-based approach to allocate resources for performing security tests on components and software from third parties. Factors that influence the risk tolerance include product deadlines, reported effectiveness of security testing, quantity of products for testing, and measuring the return on investment for security testing. According to a recent survey, 63 percent of automobile companies test less than half of hardware, software, and other technologies for vulnerabilities; 71 percent state that pressure to meet product deadlines is the primary factor leading to vulnerabilities.[9]

Supplier Cybersecurity Awareness

Upstream components suppliers, such as chip manufactures, cannot provide turnkey cybersecurity solutions because the implementation of these components in vehicles varies so widely from OEM to OEM, and even model to model. While OEMs are the final system integrators and are responsible for the majority of risks related to the end product, Tier-1 and Tier-2 suppliers must also take responsibility for cybersecurity. In a survey completed by McKinsey in 2017, only ten percent of automotive suppliers said cybersecurity ranks high on top management's agenda, compared to 35 percent of OEM top management's agenda.[10]

Long-term suppliers

OEMs have a long pedigree of sourcing materials and managing parts availability. New relationships may be necessary to stabilize the supply of some wireless transceivers. Most mobile devices, the primary market for these type of components, release new hardware on a near annual basis which contrasts with automakers that keeps parts in production for decades.

Automotive Supply Chain Risks

Two primary risks emerge as the automotive supply chain evolves. First, components such as sensor technologies and communications modules, which are necessary for vehicle automation and connectivity, may render vehicles susceptible to cyber threats by broadening a vehicle's attack surface across the supply chain. Second, new suppliers are necessary for advanced vehicles to supply software and other digital components; yet the automotive industry has been slow to establish sufficient cybersecurity protocols and guidelines with these new (or even most traditional parts) suppliers. These are elaborated upon below.

[9] Ponemon Institute, "Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices," 2019.

[10] Corrado Bordonali, Simone Ferraresi, and Wolf Richter, "Shifting gears in cyber security for connected cars," (McKinsey & Co.), February 2017, https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx

Risk Area: Malware and Contaminated Components

Throughout the automotive supply chain, materials, infrastructure, enterprises, and customers are vulnerable to a variety of attack vectors. Malware, product tampering, and other virtual disruptions are the primary software supply chain risks to vehicles and companies. If products are tampered with or contaminated upstream, compromise may occur before the vehicle reaches the road. Thus, waiting to harden the vehicle after assembly may not be adequate if contaminated components are already in vehicles. Manufacturing integrated circuits and semiconductors often occurs overseas, including China, South Korea, and Taiwan.

Recommendation: *Investments in developing an interoperable software bill of materials to detect and track changes to software will aid in attribution when threats introduce malicious code. Controls, such as separation of duty and periodic vetting of personnel and business partners, are necessary to have confidence that insiders do not cause harm. Designs should consider the use of zero trust models when there is low assurance between interfaces and there are limited alternatives to improve assurance of the subjects/assets in the architecture.*

Risk Area: Cybersecurity Guidelines

Traditional automotive standards bodies, such as Society for Automotive Engineers (SAE), have not yet published a comprehensive industry-standardized guideline for the implementation of cybersecurity. As such, each OEM and supplier vary in their approach and implementation, which introduces system-level risks.

Recommendation: *OEMs and suppliers must work together to better define cybersecurity standards in the design phase. Additionally, establishing standards for coding practices and documentation of security requirements across the automotive industry would assist in establishing a culture of cybersecurity for entities in the upstream supply chain.*[11]

[11] Bordonali, et. al., “Shifting gears in cyber security for connected cars,” February 2017.

Threat Intelligence and Detection

Cyber intelligence, threat analysis, and early detection are critical to risk management of product cybersecurity in the automotive industry. However, detection measures are only of value if proper response mechanisms are in place. Parallel maturation of automotive cyber intelligence, threat analysis and detection, and incident response is crucial to determining and addressing risks of advanced vehicle technologies.

Automotive Threat Intelligence & Detection Overview

Cyber intelligence consists of "acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making."[12] Typically, threat intelligence has been associated with the intelligence, defense, and national security community. However, this type of intelligence can be extremely valuable for individuals leading organizations in private industry, as the private sector is progressively targeted by domestic and foreign threat actors. Given the economic significance and safety implications of the automotive industry to the U.S. at large, cyber intelligence for the automotive sector is now vital to the safe incorporation of advanced vehicle technologies.

Thus, the U.S. automotive industry can particularly benefit from threat intelligence and information sharing as vehicles become more technically advanced and connected. Threat intelligence can empower automotive organizations to make informed decisions to mitigate risks associated with potential threats and vulnerabilities. Early threat detection can reduce the time that attackers have access to a system once breached, enabling a quicker response and remediation.

The automotive industry is in the process of establishing information-sharing pipelines, and there are a variety of alliances and organizations with whom automotive companies can partner with to track cyber threats to advanced vehicles. There are also a number of companies offering intrusion detection and prevention solutions, which will aide automakers in early threat detection and minimize total response time.

Some current sources for automotive-related threat intelligence are included in the Appendix to this section.

[12] Jared Ettinger, et. al., Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States, (Carnegie Mellon University Software Engineering Institute), 2019, p. 3.

Factors Affecting Automotive Threat Intelligence & Detection

As vehicle technology is increasingly computerized and digitized, and vehicles are equipped with internal and external data communications networks, the changing environment requires a better understanding of the cybersecurity risks threat landscape. However, there are some impediments to the usage of traditional cybersecurity intelligence and detection tools, listed in the table below:

Lack of Common Vernacular	There is a lack of common language to discuss cyber threats between the government and vehicle manufacturers. This can impede collaboration and communication between automobile manufactures and the government.
Organization Response Channel	Threat intelligence is most useful when organizations can quickly and efficiently turn that information into actionable steps towards mitigation. Ensuring that threat intelligence gets into the hands of individuals within the company with the ability to mitigate the threats is critical.
Challenging Remediation Environment	Remediation of cybersecurity vulnerabilities may require vehicle software updates, often involving a time-consuming, costly installation by a certified technician. In contrast, most other information systems and mobile phones, and many IoT devices, can be updated remotely.
Limited real-time threat detection adoption	Although it is common to have intrusion detection and prevention appliances deployed in enterprise information systems, this concept has not been fully adopted in vehicle networks.

Threat Intelligence & Detection Risks

Risk Area: Threshold for Action

Understanding when and how to act on cyber threat intelligence to mitigate risks associated with vulnerabilities is a challenge. Depending on the affected and vulnerable component—and where it from in the supply chain—multiple parties may need to advise on the remediation solution. As in any other advanced technology environment, not every vulnerability requires mitigation, depending on the impact and severity. Due to the cyber-physical nature of the safety-critical components, threat intelligence can indicate whether other measures may be needed to ensure that end users are not harmed by an unmitigated vulnerability. Additionally, the decision-makers within automotive companies must be sufficiently sophisticated consumers of cyber intelligence and threat analysis to reasonably determine appropriate thresholds for action. Failures in automotive cyber intelligence production and threat analysis, or in leadership's digestion of that intelligence, yield risks to accurately assessing the thresholds for action in response to threats.

Recommendation: *Automotive manufacturers and suppliers should continue to develop their firms' cyber intelligence and threat analysis capabilities, in conjunction with industry organizations and government resources. This should include leadership to prepare them for assessing appropriate actions in response to intelligence findings.*

Risk Area: Detection is key, but also useless without response

Real time detection is imperative to reducing the time attackers have access to a system after a breach. Attackers may go undetected in a system for months, and once identified the penetrated organization must move swiftly to determine extent of the compromise. This implies a need for a dedicated analysis platform to provide this level of systemic surveillance, but which automotive companies have typically not deployed to monitor in-vehicle systems. In some cases, there are efforts to join forces between enterprise IT and vehicle networks to bring these capabilities to the operational vehicle environment, and most organizations we spoke with are trying to incorporate forms of real time threat detection into their systems.

However, once a vulnerability or threat activity has been detected it also takes a fair amount of analysis to determine the impact, potential consequences, and overall level of risk to the operation of the vehicle. In parallel to improving their detection capabilities, many organizations are seeking to strengthen their incident response measures: the gap between detection and response creates risk.

Recommendation: *Incident response plans of both private and public sector entities involved with advanced vehicle technologies need to be developed and coordinated with cyber intelligence and threat analysis programs to best synchronize threat detection and response.*

Appendix to Section: Current Sources of Automotive Cyber Intelligence

ATA Fleet Cywatch

Auto-ISAC

Bug bounty programs (OEM specific, Hacker One, Bug Crowd)

Call center service support

Cyberauto challenge

Cybertruck challenge

DEFCON car hacking village

DHS AIS

DHS HSIN

Domestic Security Alliance Council (DSAC)

ESCAR Conference

InfraGard

The National Cyber-Forensics and Training Alliance (NCFTA)

Vulnerability disclosure programs

People

People are what enable continuous innovation and advancement of vehicle technology. They can also be the source of the greatest risks to vehicle cybersecurity. Appropriate leadership, organizational culture, and personnel security practices are crucial to mitigating risks associated with people in the automotive sector.

People Overview

A wide range of government, private, managerial, technical, and support personnel are involved in the advanced vehicle technology ecosystem. These people are the foundation of all advanced vehicle products, whether within the OEMs, Tier 1 and Tier 2 suppliers, or government agencies. Because humans are typically the weakest security link, their individual and collective behaviors pose increased cybersecurity risks to proprietary data, personal information, and product security.[13] Fostering a culture of shared responsibility for cybersecurity that encourages team risk management can mitigate these dangers and drive collective success.

Factors Affecting Risks Associated with People

There are two key factors that shape risk associated with people in the automotive industry.

Breadth of Engagement in Cybersecurity

Only a small percentage of automotive OEM and supplier management agendas are focused on cybersecurity, according to McKinsey.[14] Incorporating adequate cybersecurity features into increasingly complex products often is overlooked. Yet, system defects and vulnerabilities can be unwittingly created by developers or aggregated from components.[15] The fast pace of innovation and the evolving cyber threat landscape further complicate security efforts. With so little attention on product cybersecurity relative to other facets of vehicle design and production, the breadth of engagement is a condition shaping risks.

[13] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, "Insider Threat Programs for the Critical Manufacturing Sector: Implementation Guide," August 2019, https://www.dhs.gov/sites/default/files/publications/19_0830_cisa_insider-threat-programs-for-the-cm-sector-implementation-guide.pdf.

[14] Bordonali, et. al., "Shifting gears in cyber security for connected cars," February 2017.

[15] Barry Sheehan, et. al., "Connected and autonomous vehicles: A cyber-risk classification framework," Transportation Research Part A: Policy and Practice, Volume 124, June 2019, pp. 523-536, https://doi.org/10.1016/j.tra.2018.06.033.

Leadership and Organizational Culture

Leadership drives organizational cultural and can signal the importance of security for the strategic success of advanced vehicle technologies. As discussed above, organizational culture drives the product development processes and intensity of attention to cybersecurity. Accordingly, leadership can enable a strong, security-conscious culture where risk-aware behavior is the norm rather than the exception. This may ultimately lead to vulnerability identification and mitigation. Employees in many positions may have the skills or curiosity to identify risks overlooked by technical developers. Without a strong cybersecurity culture, employees may be reluctant to contribute beyond their normal job roles.

Automotive Risks Associated with People

Risk Area: Malicious and Insider Threats

Technical controls, risk programs, and investigations are not enough to protect advanced vehicle technology. The people who support the advanced vehicle technology ecosystem should understand how human behavior contributes to product cybersecurity vulnerabilities. Employees, contractors, vendors, and other trusted third parties all can create risk. Disgruntled employees can conduct malicious acts to sabotage information, networks, and products. For example, as early as 2010, a disgruntled former employee of a car dealership “bricked” over 100 cars sold by the dealership using access to a web-based service that is an alternative to repossessing vehicles.[16]

More commonly, human error unwittingly creates vulnerabilities that expose the company to external risks.[17] For example, poor security practices or weak security protocol enforcement can leave an organization vulnerable to social engineering techniques or a computer network attack that results in data, financial, or reputational losses. Nonetheless, insider threat incidents are increasing and remediation after the fact is always the most expensive response.[18]

Recommendation: *Human Resources (HR) departments can sensitize employees to insider threats. Information Technology departments can work with HR to proactively monitor suspicious employee behavior and prevent or deter malicious activity before employee termination.*

Risk Area: Unidentified or Unexplored Vulnerabilities

All of the people who support the advanced vehicle technology ecosystem should participate

[16] Kevin Poulsen, “Hacker Disables More Than 100 Cars Remotely,” Wired, March 17, 2010, https://www.wired.com/2010/03/hacker-bricks-cars/.

[17] Tucker Bailey et. al., “Insider threat: The human element of cyber risk,” (McKinsey & Co.) September 2018, https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk.

[18] https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf

in risk reduction initiatives to protect products and information. Risk management is an important strategy that can empower people to proactively identify vulnerabilities and mitigate potential consequences before they occur. McKinsey recommends identifying and prioritizing key business capabilities or information to protect, determining which employees have access, and developing a risk-based, prioritized identification and protection process.[19] Otherwise, cybersecurity vulnerabilities may go unnoticed, without being recognized or addressed.

Recommendation: *To identify, detect and mitigate cybersecurity risks before they cause harm, the industry and organizational cultures should empower employees at all levels with the shared responsibility for cybersecurity. Encouraging all employees to contribute to cybersecurity discussions reinforces their value and builds stronger teams. To further this aim, HR can embed cybersecurity awareness into employee recruiting and training*.

[19] Bailey, "Insider threat: The human element of cyber risk," September 2018.

Education

Cybersecurity awareness and training programs enable advanced vehicle technologies and must go beyond the traditional educational model. The success of these efforts benefit from executive support and information sharing outside the organization.

Education Overview

Before the modern connected and automated vehicle, engineers of safety-critical components delivered mechanical capability, without the threat of cyber-attack. With increased connectivity and automation, engineers must now expand their aperture to consider the cybersecurity threat landscape in their designs. Each product team member requires at least a basic knowledge of how to build a secure system for advanced vehicle technologies.

There are two parts to a proper security education program: (1) Awareness and (2) Training. According to the Automotive Information Sharing and Analysis Center, “A cybersecurity awareness and training program is an organizational capability designed to improve the cybersecurity knowledge and mindfulness of employees and partners to reinforce positive cybersecurity practices.“[20]

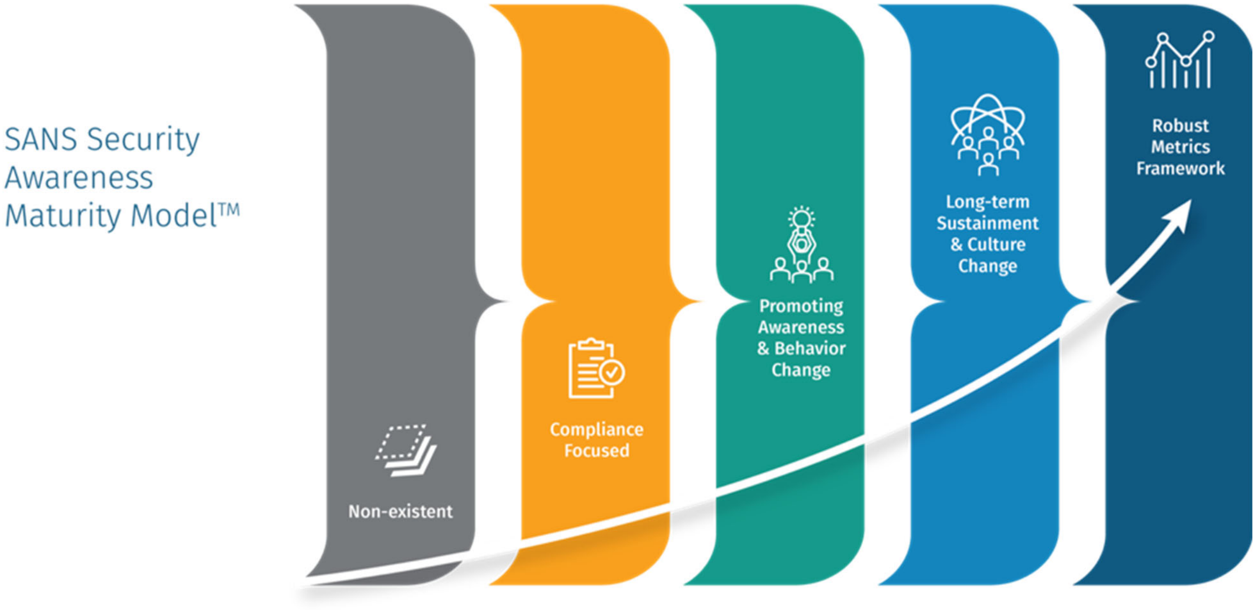
Thus, organizational culture is the key to a successful program. No matter how many training courses, policies or metrics the company is tracking, the culture must embrace continuous learning. Changing the culture of a well-established or large organization can be daunting, and the design of the security awareness and training program should be thought through as well.

The Security Awareness Maturity Model, shown below, is well explained by SANS. This model shows the stages through which a company must pass, as well as metrics to achieve, in order to reach full maturity in their company culture of security.[21]

[20] Auto-ISAC, “Awareness and Training Best Practice Guide, Version 1.3,” August 19, 2019, p. 3, https://www.automotiveisac.com/best-practices/download-best-practice-guides/.

[21] Lance Spitzner, “The SANS Security Awareness Roadmap,” (website), July 30, 2019, https://www.sans.org/security-awareness-training/blog/sans-security-awareness-roadmap.

Figure 1: SANS Security Awareness Maturity Model^{TM}


SANS Security Awareness Maturity Model™
Non-existent
Compliance Focused
Promoting Awareness & Behavior Change
Long-term Sustainment & Culture Change
Robust Metrics Framework

Factors Shaping Automotive Cybersecurity Education

There are several key factors that affect risks associated with cybersecurity education in the automotive industry, described below.

Overcoming legacy behaviors — Experienced automotive engineers now require new technical skills and approaches to building secure products, beyond their traditional role or expertise. The dynamic nature of cybersecurity is also a significant evolution from industry requirements.

Misconception that security is a niche expertise — Cybersecurity cannot be embedded into the architecture, system, component, or feature by experts alone. Everyone involved in product development, including non-technical roles, needs to have a basic understanding of security and what role they play in delivering a secure product.

Lack of industry-specific training resources — During our interviews, it was clear that organizations with executive commitment to security education had more robust and mature security postures overall. Organizations with lower levels of support have a more difficult time building their security programs. As security does not directly affect revenue growth, education can too easily be deprioritized relative to other development initiatives.

Limited institutionalized education programs	Automotive cybersecurity degrees and formal training programs are still being developed by higher education institutions. Top candidates in this specialty do not typically learn these skills in a classroom, but rather through their own investigations and interests. This makes finding candidates through traditional recruiting and hiring practices more difficult.

Education Associated Risks

Risk Area: Education on Cybersecurity is Ever Evolving

Due to the dynamic (and sometimes reactionary) nature of cybersecurity, education programs need continuous updating to stay relevant in this field. There are new vulnerabilities and threats being discovered every day, so it is important to stay current. It is truly a job that is never complete.

Recommendation: *The success of cybersecurity education relies on continuous learning from information sharing, networking and conferences, as well as training. Organizations like the Automotive-ISAC are a key piece of keeping the automotive workforce current.*

Risk Area: Workforce Educational Maturity is an Evolution, Not a Revolution

With the rapid advancements in the automotive industry, innovation is outpacing workforce education on cybersecurity. However, setting up an education program today does not immediately benefit products in the marketplace. With the need to educate not only the legacy workforce, but also initiate a pipeline for entry-level candidates through institutionalized education programs, the industry security awareness model is still in its infancy.

Recommendation: *Persistence and patience are key to long term support for requisite cybersecurity educational programs. Establishing such programs with an eye toward developing and sustaining a talent pipeline will aid the automotive workforce over the long run.*

Public Policy

Public policies, while often expected to provide improved cybersecurity measures, can actually create new risk areas which industry will be limited in mitigating.

Automotive Public Policy

The public policy environment for advanced vehicle technologies is complicated and encompasses a wide range of governments and governmental actors. Policymakers at the Federal, state, and local levels address aspects of legislation and/or regulation that impact vehicles and vehicle technologies. Governments also conduct research, provide funding for other entities' research and deployment of technologies, convene multistakeholder processes and discussions that address issues of concern, and levy enforcement (civil or criminal) against entities alleged to violate laws or regulations. And since the automotive industry is global, foreign countries and regional organizations also promulgate influential policies toward advanced vehicle technologies. Each of these governmental actions help shape the decision making of industry participants developing, deploying, and in some cases operating advanced vehicle technologies with regard to vehicle cybersecurity. Thus, public policy is an important area for assessing risks.

Policy-derived risks to vehicle cybersecurity emanate from three primary categories of policies — restraints, constraints, and policy coordination:

- Policy **restraints** limit the ability of developers and providers of vehicle technologies to effectively reduce cybersecurity vulnerabilities in their products. These establish what industry cannot do.
- Policy **constraints** require or encourage actions by providers of vehicle technologies that contribute to the creation of cybersecurity vulnerabilities. These establish what industry must do.
- Policy **coordination** risks stem from difficulties in developing and implementing policies, whether by a single governing entity or through collaboration between entities with shared jurisdiction. These may result in duplication of, conflict between, or gaps in policy measures addressing advanced vehicle technologies. In turn, these deficiencies may reduce the ability to efficiently take steps to reduce vehicle cybersecurity vulnerabilities.

Risks of these sorts will often be unintended effects of policies aimed at achieving some other policy objective.

A fourth category of policy-related risk to vehicles, albeit one beyond the scope of this report, pertains to government actions taken (or not taken) to defend against threat actors that may seek to exploit the cyber domain to attack vehicle vulnerabilities for malicious ends.

Factors that Lead to these Restraints, Constraints, and Coordination Challenges

There are three factors that create the public policy challenges for addressing vehicle cybersecurity, described below.

Jurisdictional Complexity and Ambiguity

While it is clear and well accepted that the U.S. Department of Transportation (DOT), through the National Highway Traffic Safety Administration (NHTSA), has regulatory and enforcement jurisdiction over safety related matters involving cars and trucks, there are subtleties to jurisdictional concerns involving the cybersecurity of advanced vehicles.[22] The technical difficulties associated with determining when a vehicle cybersecurity vulnerability may pose a potential impact to vehicle safety produce a degree of uncertainty about when such a vulnerability actually constitutes "a defect related to motor vehicle safety."[23] That is the necessary condition for the exercise of Federal motor vehicle safety authority over the cybersecurity vulnerability. Motor vehicle safety is defined in statute as:

> …the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle.[24]

Because a cybersecurity vulnerability must be exploited by an actor to produce an actual *consequence*—i.e. a "risk of accident occurring"—even[25] a vulnerability that may have a nexus to the safe operation of a vehicle may not pose a safety hazard absent such malicious exploitation. And that exploitation would in most circumstances, other than limited research efforts, be a crime subject to criminal enforcement against the threat actor. This complicates the assessment of the legal and regulatory status of cybersecurity vulnerabilities.

Another dimension of the jurisdictional complexity results from Federalism. Because vehicles

[22] NHTSA has stated: "Vehicles are cyber-physical systems and cybersecurity vulnerabilities could impact safety of life. Therefore, NHTSA's authority would be able to cover vehicle cybersecurity, even though it is not covered by an existing Federal Motor Vehicle Safety Standard at this time." National Highway Traffic Safety Administration, Cybersecurity Best Practices for Modern Vehicles (Report No. DOT HS 812 333), Washington, DC: October 2016, p. 5.

[23] 49 U.S.C. §30118(a).

[24] 49 U.S.C. §30102(a)(9).

[25] 49 U.S.C. §30102(a)(9).

are introduced into interstate commerce by the automotive OEMs, the vehicles are subject to Federal authority. But the operation of the vehicles, and thus the conditions and requirements for using them on roads, are subject to state jurisdiction and policies addressing titling, licensing of operators (human or automated driving system), insurance requirements, and traffic laws. Similarly, roadside infrastructure to which vehicles may connect (e.g. for vehicle-to-infrastructure ("V2I") connectivity and integration with "smart city" technologies) is typically owned, operated, and/or controlled by state or local governments. Often this state/local control is significantly influenced by Federal policy through funding, research and development, and other road operation resources provided by U.S. DOT and the Federal Highways Administration (FHWA). Thus, cyber infrastructure that may be communicating with vehicles may be controlled by thousands of different governmental entities.

Additionally, vehicles with connectivity are endpoint devices for the Internet of Things. Laws, regulations, and other policy actions that are intended to address the "Internet of Things" generically, or "connected devices" may, intentionally or inadvertently, include vehicles within their definitions. This further complicates the policy environment for advanced vehicle technologies by potentially subjecting it to duplicative yet conflicting requirements: those specific to vehicles and those generic to "connected devices."

Competing Policy Objectives

In addressing advanced vehicle technologies and vehicle cybersecurity, policymakers generally seek to balance several objectives that at times may be in tension with one another. These include encouraging technology innovation and economic growth, improving transportation safety and efficiency, and assuring security and privacy in service of the public interest. Additionally, policymakers often seek to balance the interests of a range of constituencies pertinent to the extended automotive industry, including consumers and the general public, automotive manufacturers and suppliers, car dealerships, independent/third party automotive repair businesses, trial lawyers, and insurance companies. Each of these groups affects and is impacted by automotive cybersecurity in some way. Policies favored by one group for its own parochial interests may aide in improving automotive cybersecurity or may contribute additional risks to automotive cybersecurity. Accordingly, the balances struck by policymakers between these stakeholders will impact vehicle cybersecurity.

Automotive Cybersecurity Technological Complexity and Speed of Innovation

The technical details of automotive cybersecurity make policymaking challenging. While some interested parties have advocated for draconian approaches to achieve safety from exploitations of cybersecurity vulnerabilities,[26] the cost-benefit standards required for regulatory rulemakings can

[26] See, e.g.: Consumer Watchdog, "Kill Switch: Why Connected Cars Can Be Killing Machines And How to Turn Them Off," July 31, 2019, https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf.

make such approaches difficult to justify. Many technologies that could potentially have cybersecurity deficiencies provide key safety improvements in normal vehicle operations. These include Advanced Driver Assistance Systems (ADAS) that provide features like Forward collision warning plus autobrake (up to 50% crash reduction), Rear automatic braking (up to 78% crash reduction), and Lane departure warning (up to 21% injury crash reduction).[27] Weighing the totality of the benefits of advanced vehicle technologies against the totality of the potential costs is difficult, and involves some inherent uncertainties.

Public Policy Risks

Policy Risks from Restraints

Risk Area: Exemptions to Prohibition Against Circumvention of Technological Protection Measures ("TPMs") Protecting Copyrighted Works under the Digital Millennium Copyright Act ("DMCA").

The Digital Millennium Copyright Act ("DMCA," 17 U.S. Code §1201) prohibits circumventing TPMs that prevent unauthorized access to copyrighted works, including computer software.[28] Every three years, the U.S. Copyright Office engages in a rulemaking proceeding to assess proposed exemptions to the prohibition on circumvention of protections for certain classes of copyrighted works. In each of its last two triennial reviews (2015 and 2018), the Copyright Office has considered proposed exemptions to TPMs protecting automotive computer code.

In 2015, the Copyright Office considered a proposed "Class 21"[29] of exemptions that would have rendered legal the act of defeating cybersecurity measures implemented in vehicles by manufacturers to protect code—so long as it was only for the limited purposes of diagnosis and repair or aftermarket personalization, and performed by the legal owner or on the owner's behalf.

The auto industry strongly objected to the proposal, expressing concerns about potential impacts to vehicle safety and emissions. The Environmental Protection Agency (EPA) was also opposed to the exemption, arguing it would enable violation of emissions standards under the Clean Air Act. The Department of Transportation (DOT) expressed serious reservations tied to both safety and emissions, while the National Telecommunications and Information Administration (NTIA) within the Department of Commerce fully supported the proposed exemption.

This was a prime example of competing policy objectives and priorities across various

[27] Insurance Institute for Highway Safety, "Real-world benefits of crash avoidance technologies," June 2019, https://www.iihs.org/media/259e5bbd-f859-42a7-bd54-3888f7a2d3ef/e9boUQ/Topics/ADVANCED%20DRIVER%20ASSISTANCE/IIHS-real-world-CA-benefits.pdf.

[28] U.S. Copyright Office, "Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works," (website), https://www.copyright.gov/1201/2018/.

[29] Federal Register Vol. 80, No. 208 October 28, 2015, available at https://www.copyright.gov/fedreg/2015/80fr65944.pdf, at 65954-65955.

policymaking entities with differing jurisdictions impacting vehicle cybersecurity. The Copyright Office sought to balance these tensions and, in light of the concerns raised by auto manufacturers, the EPA, and DOT, issued a final rule that approved the exemption but narrowed it and delayed its implementation. The key limitation was that the exemption did not cover vehicle telematics or entertainment systems.[30] The delay was intended to allow DOT and/or EPA to issue any additional rules addressing their concerns.

In 2018, the Copyright Office again considered a similar class of exemptions. Proponents of the exemptions argued the 2015 exemption should be renewed and expanded to include exempting circumvention of TPMs protecting telematics and entertainment systems ECUs, and to remove the requirement that such circumvention be performed by an authorized owner of the vehicle. The Acting Registrar agreed and recommended an expanded exemption.[31]

These exemptions to the DMCA provide a degree of protection for the creation of tools that can defeat vehicle cybersecurity protection measures. While there are legitimate public interests in these exemptions, they also create risks by permitting the development of tools that may spread beyond their intended uses and users.

Recommendation: *Future triennial DMCA exemption reviews should more seriously weigh the potential adverse consequences defeating vehicle cybersecurity measures and refrain from extending or expanding these exemptions.*

Policy Risks from Constraints

Risk Area: OBD-II Port Requirement

Beginning in 1996 and in successor regulations, the Environmental Protection Agency (EPA required the implementation of the On-Board Diagnostic Port (OBD and its successor OBD-II port.[32] This port enabled access to a range of diagnostic and repair information, as well as a variety of third-party devices services.providing additional in-vehicle capabilities.[33] However, the OBD-II port also provides a potential vector for cybersecurity breaches of vehicle architecture, if attached devices are not properly secured.[34]

[30] Federal Register Vol. 80, No. 208 October 28, 2015, available at https://www.copyright.gov/fedreg/2015/80fr65944.pdf, at 65954-65955.

[31] Section 1201 Rulemaking: Seventh Triennial Proceeding Recommendation of the Acting Register of Copyrights, October 2018, p. 184-230.

[32] 40 C.F.R. Part 86. See also: Federal Register, Vol. 60, No. 153, August 9, 1995, 40474.

[33] See, e.g., "Harman Spark," (website), https://services.harman.com/microsites/att-harman-spark.

[34] Team discussions with various automotive industry subject matter experts Note, the Harman Spark product was the first IoT device to pass CTIA's IoT Device Security Certification.

Recommendation: Policymakers, in coordination with industry, should assess the continued relevance and importance of the OBD-II port requirement balanced against cybersecurity concerns.

Risk Area: "Right-to-Repair" requirements.

Closely related to both the OBD-II requirement and the DMCA exemptions is the concept of "right-to-repair."[35] The OBD-II port enabled a broad range of third parties to access vehicle diagnostic information. This has supported independent repair shops' abilities to diagnose and repair vehicles as they have grown more technologically complex. In recognition of the potential cybersecurity vulnerabilities associated with the OBD-II port and access to repair and diagnostic information, automotive OEMs have sought to limit access to that information to trusted and authenticated entities.[36] Advocacy groups have pushed many states to consider legislation requiring automotive OEMs to enable access to vehicle repair and diagnostic information and architectures to third parties, in the belief that vehicle owners should have the "right to repair" their vehicles in the manner of, and by the entities, of their choosing. Increasing access to vehicle cyber systems increases the risk of exploitation of potential vulnerabilities.

Recommendation: *Right to repair advocates should work with the automotive industry to address remaining concerns with a concerted focus on the cybersecurity implications of opened access to vehicle architectures. Legislators should refrain from mandating access to vehicle architecture in ways that create cybersecurity vulnerabilities.*

Risk Area: Electronic Logging Device (ELD) Mandate

In 2012, Congress required that the USDOT, through the Federal Motor Carrier Safety Administration (FMCSA), introduce a mandate to track truck drivers' hours-of-service electronically. The subsequent rule replaces legacy solutions like on-board computers and paper -based logs.[37] The rule requires that the ELDs "synchronizes with the [commercial motor vehicle] engine" to record data pertinent to the hours-of-service logging.[38] However, the rule does not specify a minimum level of cybersecurity protection for ELD products. Poorly secured ELD products can expose commercial vehicles to potential threats that the vehicles were not initially designed to address.

Recommendation: *Industry should develop a voluntary labeling program designed to provide information to the commercial motor vehicle community using ELDs about ELD products, including their assessed level of cybersecurity assurance based on risk.*

[35] See, e.g., The Repair Association, Legislation, https://repair.org/legislation.

[36] See, e.g. National Automotive Service Task Force (NASTF), https://www.nastf.org/.

[37] Federal Motor Carrier Safety Administration Final Rule, Federal Register, Vol. 80, No. 241, December 16, 2015, https://www.govinfo.gov/content/pkg/FR-2015-12-16/pdf/2015-31336.pdf.

[38] Federal Motor Carrier Safety Administration, "About ELDS: Improving Safety Through Technology" (website), https://eld.fmcsa.dot.gov/About.

Policy Risks from Coordination

Risk Area: Impact of NHTSA Safety Jurisdiction on Cybersecurity Information Assessment and Sharing

NHTSA's statutory authority under the Motor Vehicle Safety Act addresses safety issues but does not currently specifically address cybersecurity. The Cybersecurity Act of 2015 improved the private sector's ability to share cybersecurity information, but (a) was not oriented on the peculiarities of the automotive industry and (b) was limited in the expansion of the exemptions and protections afforded industry.[39]

This results in NHTSA and industry operating under a degree of regulatory uncertainty regarding the scope of NHTSA's regulatory authority pertaining to vehicle cybersecurity. In turn, this inhibits information sharing within the industry that could improve the cybersecurity posture of the industry.

Recommendation: *Federal policymakers should expand the protections encouraging cybersecurity information sharing provided by the Cybersecurity Act of 2015 and provide tailored solutions to the regulatory overhang concerns that impede automotive cybersecurity information sharing.*

Risk Area: Lack of a Connected and Automated Vehicle (CAV) Subsector and Corresponding Government Coordinating Council and Sector Coordinating Council for CAVs.

Within the Federally designated sixteen critical infrastructure sectors as defined in Presidential Policy Directive-21,[40] the Transportation Systems Sector currently encompasses seven subsectors. These are: aviation, highway and motor carrier, maritime, mass transit and passenger rail, pipeline, freight rail, and postal and shipping.[41] While the highway and motor carrier subsection addresses protection of road infrastructure and the associated and supporting cyber infrastructure enabling road operations, none of these seven subsectors covers connected and automated vehicles.

Recommendations:

1. *Designation of Connected and Automated Vehicles as an eighth subsector of the Transportation Systems critical infrastructure sector.*

2. *Establishment of Connected and Automated (CAV) Vehicle Subsector Government Coordinating*

[39] Megan Brown, "Cyber Imperative: Preserve and Strengthen Public-Private Partnerships," The National Security Institute White Paper, October 11, 2018, p. 13, https://nationalsecurity.gmu.edu/cyber-imperative-preserve-and-strengthen-public-private-partnerships/.

[40] Daily Comp. Pres. Docs., 2013 DCPD No. 00092, "Directive on Critical Infrastructure Security and Resilience (PPD-21)," February 12, 2013, https://www.govinfo.gov/content/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf

[41] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, "Transportation Systems Sector," (website), https://www.dhs.gov/cisa/transportation-systems-sector#.

Council (GCC) and Sector Coordinating Council (SCC).

Flowing from the designation of CAVs as a transportation systems subsector of critical infrastructure, DHS and DOT, as co-Sector Specific Agencies for transportation should establish both a Government Coordinating Council (GCC) and a Sector Coordinating Council (SCC) for CAVs. These councils would facilitate government and industry collaboration on CAV subsector-specific risks, especially cybersecurity risks to (and from) advanced vehicle technologies. The quadrennial update of the sector-specific plan for transportation should incorporate these changes in recognition of the rapid advancement of CAV technologies and their potential impact on U.S. critical infrastructure.

Risk Area: Lack of establishment of SCMS governance model for V2X communications security.

The Secure Credential Management System (SCMS) is the envisioned security architecture undergirding the integrity, authenticity, and privacy of V2V and V2I messages. It is a large-scale Public Key Infrastructure (PKI) solution that requires a number of different functions to be enabled by a variety of parties.[42] These include PKI certificate issuance and distribution, misbehavior detection and revocation, and root certificate management. Coordination of all of these functions nationally requires an overarching, systemic governance model. Such a model is currently undetermined.[43] Delay or failure to establish a scalable governance model will delay or prohibit the broad deployment of V2X communications and the attendant safety benefits. Alternatively, a flawed governance model could create new security risk areas.

Recommendation: *USDOT/NHTSA should continue to lead stakeholders toward development and establishment of a functional model that meets technical and business requirements.*

[42] Bob Kreeb, "Next Steps for Deploying a National Security Credential Management System for V2X Communications,"

https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/sae2018rkreeb.pdf.

[43] Kreeb, "Next Steps for Deploying a National Security Credential Management System for V2X Communications," 2018.

Conclusion

The report has attempted to provide a high-level survey and categorization of risks associated with advanced vehicle technologies. The topic is as broad as the industry itself and the array of potential vulnerabilities and threats it faces. Cooperation within and across the industry, with academia and research institutions, and with public sector partners in a diverse set of agencies, is necessary to continue to address the challenges presented by these advanced technologies.

Future research efforts may seek to refine selected categories presented here, and to further develop our understanding of the potential vulnerabilities, threats, consequences, and resultant risks.