

HOW WILL GOVERNMENTS REGULATE AUTOMOTIVE CYBERSECURITY?

by

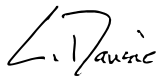
Alex Hewitson

A Senior Honors Thesis Submitted to the Faculty of
The University of Utah
In Partial Fulfillment of the Requirements for the
Honors Degree in Bachelor of Science

In

Information Systems

Approved:



Chris Dansie
Thesis Faculty Supervisor



Glen Schmidt
Chair, Department of Operations and
Information Systems



Vandana Ramachandran
Honors Faculty Advisor

Sylvia D. Torti, PhD
Dean, Honors College

ABSTRACT

Digital attacks are becoming vastly common, and global events like the COVID-19 pandemic only press the accelerator pedal further. Cybersecurity regulations enforce security standards for a given industry but are slow to do so for emerging vulnerabilities. The automotive industry is a novel and critical example as vehicles become increasingly connected to and dependent on the internet. This paper addresses the need for global, rather than currently regional, regulation of automotive cybersecurity. Considering the immense risks of user information, particularly location data, and even compromising a driver's control of a vehicle, the paper explores the challenges of regulating companies from around the globe to mitigate such risks. Through synthesizing existing regulations, regulations of other industries, and the present threat landscape, the paper reports on the gap between current automotive cybersecurity regulations and what is necessary to best maintain the confidentiality, integrity, and availability of information produced and accepted by connected vehicles. The paper stresses the implications of such attacks and their scale, which incorporates not only those in a connected vehicle but also those sharing the road and the nearby area. Findings include how global cybersecurity regulations in other sectors may apply to automobiles, the nuances of regulating the industry, and key recommendations.

TABLE OF CONTENTS

ABSTRACT	ii
INTRODUCTION	1
OVERVIEW OF AUTOMOTIVE CYBERSECURITY	3
CURRENT REGULATORY FRAMEWORK	7
REGULATIONS FOR OTHER SECTORS	10
KEY PLAYERS AND STAKEHOLDERS	13
CHALLENGES	17
PROPOSED REGULATORY APPROACHES	21
CASE STUDIES	25
RECOMMENDATIONS	28
CONCLUSION	33
REFERENCES	36

INTRODUCTION

Are drivers always in control of their vehicles? Personal vehicles are rapidly evolving into internet-connected devices capable of receiving software updates, connecting to the traffic grid system, other vehicles, and more (Lu et. al, 2014). This new wave of automotive technology presents exciting safety advantages, as vehicles become more aware of their surroundings, such as the next traffic light's status. However, there are also new concerns to address. As the next subject of infusion with technology, connecting cars to the internet presents a unique threat landscape. Manufacturers have proprietary vehicle control systems that are seldom available for third-party researchers to investigate, making it difficult to identify and mitigate vulnerabilities. Furthermore, the complexity of new vehicles makes them more difficult to maintain and more susceptible to network outages. Most concerningly, connecting vehicles to the internet exposes them to cyberattacks. Threat actors can install malware on a car's system, causing it to malfunction or lose control. Attacks can also fool the vehicle or its driver into disclosing sensitive information such as login credentials or payment details on vehicles with subscription-based features or integration with charging networks. Furthermore, a threat actor can compromise a vehicle to steal sensitive data such as location data or even manipulate the car's movements on the road.

Such dire implications call for clear, calculated mitigation steps to maximize the safety benefits of connected vehicles while minimizing the negative consequences, particularly cybersecurity concerns. Also, the auto industry is unique in that car factories and suppliers are widely spread throughout the globe. Data sovereignty laws state that

organizations must abide by the regulations of the country in which they store data, allowing for different controls depending on the country's use cases. However, cars collecting this data which are made in any country may be internationally distributed. If a vehicle made in one country is sold in another and collects user data, what regulations must it abide by? These concerns must be addressed uniformly since the international transfer of automobiles and their components cannot solely reside in each manufacturer's country. There is a need for widespread regulation so any vehicle capable of connecting to the internet meets the same requirements regardless of where it was made or sold.

The purpose of this paper is to begin exploring how governments and organizations could approach establishing such widespread regulation. Investigating existing automotive cybersecurity policies will establish a baseline. Then, examining other industries which demanded cybersecurity regulation in their infancy will highlight the current gaps and provide hindsight into the successes and shortcomings of establishing new information security policy for an emerging industry that is newly integrated with technology. The paper will then analyze the stakeholders of connected vehicles and their respective desires and concerns. It will finish by discussing different approaches to regulation, a look into regulation in different world regions, and recommendations for new regulation. Ultimately, the paper seeks to answer the question of how governments will regulate cybersecurity in cars as they become increasingly more dependent on the internet. With such worrying risks of cyberattacks on vehicles that impact the safety of occupants and any other road user, this issue must be at the forefront of the ongoing development of such vehicles to ensure road safety in the digital age.

OVERVIEW OF AUTOMOTIVE CYBERSECURITY

The initial development of cybersecurity concerns began in the early 2010s when security researchers reported vulnerabilities in vehicles with a 4G LTE cellular connection for in-car Wi-Fi (Hayes, 2020). Once the world took note of this novel series of attacks, others found similar vulnerabilities in the digital protection of vehicle control systems. This news initially shocked manufacturers and worried them because most have development cycles of several years for new models. They are unable to quickly develop new, secure computers and immediately install them on new vehicles. Cars are not comprised of easily swappable systems. Each digital component serves a specific purpose and cannot be merely switched to a more secure version. This trend will continue as more modern vehicles patch these initial vulnerabilities but also create new ones with connected features beyond in-car Wi-Fi such as over-the-air updates. Their attack surface only increases.

To start discovering these vulnerabilities, automakers began to implement bug bounty programs, where ethical, white-hat hackers receive a reward for discovering and reporting new vulnerabilities. General Motors and what is now Stellantis pioneered such programs in 2016 with Ford following in 2019, all of which preferred to handle the vulnerabilities internally. Tesla took a divergent approach and held public hacking contests at cybersecurity conventions, even providing a Tesla Model 3 as a reward. Their goal was to face this issue head-on and make consumers feel more confident in the product. Ultimately, major car makers waited several years after initial reports to invest great resources in hardening their products (Hayes, 2020).

Today's cars have numerous threats and vulnerabilities compromising the safety, security, and privacy of their owners. A study by Strobl et al. categorized the components of a connected vehicle into four major sectors. In-vehicle elements make up the physical car and include its controls, computers, sensors, and all input and output devices. In-vehicle cloud concerns any cloud storage or processing the vehicle needs to function. Mobile devices and outside software include devices that communicate with the vehicle. For example, some vehicles accept a digital key on the owner's smartphone as valid authentication to enter and operate it. Lastly, communication channels are the links between each component within and outside of the vehicle. They exchange any information between the previous three components. These discrete systems have their respective security concerns and must be individually hardened (Strobl et. al, 2018).

An example of a threat relating to in-vehicle elements involves electronic control units (ECUs). Although they are extremely difficult to remove and fully enclosed, they still provide diagnostic access to technicians. Therefore, they have an attack surface and if exploited, may severely affect the vehicle's movements. Connecting to services outside the vehicle poses different threats. The average age of a vehicle in the United States is over eleven years old, which includes the wireless gateways within the cars. Running outdated hardware will eventually render the vehicle unable to receive security updates with new wireless communication standards such as WPA3 for Wi-Fi. A threat actor need not spend intense resources to discover new vulnerabilities since vehicles currently on the road have well-documented weaknesses (Bécsi et. al, 2015). These threats and vulnerabilities represent a small subset of risks that can lead to dire consequences for modern society.

Unlike other technology sectors, cyberattacks on connected vehicles cause disastrous consequences in the cyber-physical realm since connected systems control the movement of a several-ton piece of machinery. Even those without connected vehicles are at risk as pedestrians, cyclists, or city dwellers. The implications of connected vehicles can affect nearly any individual in modern society, as will be described later. With vehicles becoming increasingly connected to the internet with remote access features, they become ever more available for a remote attack with the ability to interfere with the driver's control over a vehicle or steal sensitive information (Parkinson et al., 2017). The real-world safety risks to large populations that arise from attacks that involve compromising and overtaking control of a passenger vehicle or preventing its movement require no speculation.

A Study by Vivek et al. (2019) analyzed the magnitude of denial-of-service attacks on road cars. They built a digital model of the streets of Manhattan in New York City. They found that halting thirty percent of vehicles on the road during a normal day would cause a complete gridlock, cutting off access to emergency services such as hospitals, fire, and police. They also found that an adversary only needs to compromise the security of two major car brands to achieve a minimum ninety-five percent probability of gridlock (Vivek et al., 2019). Such an attack may not be feasible today as older cars from these manufacturers without connected features still account for a significant percentage. However, assuming the average vehicle age stays mostly constant, such an event can occur in the future. The United States is particularly vulnerable to denial-of-service attacks on cars due to its uniquely strong reliance on them rather than a mixed transportation system featuring alternate methods such as passenger rail.

The threats of connected vehicles do not only concern the cyber-physical realm. Risks to the vehicle owner's privacy are also prevalent. Threat actors find great value in a victim's location data. Accessing a vehicle's location can provide information for targeted theft, such as just after the victim visits a bank or a store carrying luxury goods. Attackers also have several ways to discover a victim's home address whether it is stored in the navigation system or by monitoring where the car is parked at night most frequently. Furthermore, non-criminal privacy considerations arise with connected vehicles. How and where an individual uses their car can be immensely valuable information for advertisers. For example, shopping and food chains would be highly interested in where customers go before and after visiting their locations. Advertising agencies are then able to collect more intimate data on each connected vehicle owner. Ultimately, these cars raise numerous concerns about physical security and digital privacy from both adversarial and non-adversarial perspectives (Parkinson et al., 2017).

Considering the initial development, threats, and risks of automotive cybersecurity, strong, international regulations on car manufacturers will enable the benefits of connected vehicles while best protecting their owner's safety, security, and privacy. By enforcing minimum security requirements, modern cars will remain safe regardless of their location on the planet. Some regulations in this field exist but are in their infancy as discussed below. Regulatory bodies may also adapt existing cybersecurity policies to the automotive industry. These solutions still lack a uniform approach across the globe. Such an approach is needed due to cars being produced and distributed in many different countries. This paper will address such questions and issues with regulating connected vehicles moving forward.

CURRENT REGULATORY FRAMEWORK

To thwart some of these risks held by owners of connected vehicles, automotive cybersecurity standards are under construction. A notable entrant is the ISO/SAE 21434:2021 standard released in August of 2021. The International Organization for Standardization (ISO) is a non-governmental international organization comprised of 167 standards bodies. It is responsible for several standards within the cybersecurity sector (ISO, 2021). SAE International is a professional organization of engineers and technical experts in the transportation industry (SAE, 2023). These organizations collaborated to form this framework for car manufacturers and their suppliers.

The resulting standard provides guidelines for cybersecurity culture and policies in creating connected vehicles and the sensitive components within. Its creators knew that supply-chain attacks on connected vehicles were likely due to the notably sensitive supply chains of original equipment manufacturers as seen in the microprocessor shortage (Trovao, 2020). With this knowledge, the standard does not entirely focus on the manufacturers themselves, but instead focuses on any company that produces or handles a digital component of a connected vehicle.

However, this standard is a framework of high-level goals. It does not provide details on checkpoints toward meeting the standard nor specific desired outcomes (Costantino et al., 2022). To solve this issue, other organizations have voluntarily proposed methodologies and even proprietary solutions to align with this standard. However, their efforts are purely voluntary and questions such as how the vehicle interacts with vehicular networks remain unanswered (Costantino et al., 2022).

In addition to standards like ISO/SAE 21434:2021, automotive companies also have the incentive to self-regulate. The impact of a cyberattack on any company has far-reaching consequences including, but not limited to a halt in business operations, cost of recovery, insurance cost rises, and reputation. Therefore, modern organizations have a desire to best protect themselves from cyber incidents to avoid the costly results that ultimately affect their bottom line.

Methods of self-regulation widely vary depending on the organization's threat landscape. Manufacturers commonly implement an in-house cybersecurity policy to govern company culture and procedures. Such a policy can benefit the protection of connected vehicles since it reduces the likelihood of a threat actor gaining sensitive access such as diagnostic backdoors to vehicles (Hugot et al., 2019). Organizations may also conduct internal or third-party audits of their security posture per their security policy or outside standards like ISO/SAE 21434. They may have the incentive to publicly display compliance with such frameworks to increase their reputation. Incident response plans are another critical element of self-regulation in the automotive industry because car brands in particular must be prepared to minimize the damages of a cyber-incident. There is a degree of understanding that adversaries can be highly funded and even state-sponsored. Therefore, automotive companies must not assume that their security controls are foolproof. Being able to quickly stop an attacker after a breach is essential to road safety since each vehicle within a brand has a copy of the hardware and software of others, meaning that lateral movement may be trivial. These forms of self-regulation protect the companies themselves and their customers but are ultimately unenforceable on an industry-wide basis.

Governments are just beginning to regulate cybersecurity in the automotive industry. The United States, however, is behind governments like South, Korea, Japan, and the European Union. There is currently no specific regulation for cybersecurity in passenger vehicles. The National Highway Traffic Safety Administration (NHTSA) updated its best practices for cybersecurity in modern vehicles, but the document is not enforceable. It serves as an optional tool for domestic car makers to follow if they need additional guidance (NHTSA, 2021).

Other regions abide by the United Nations Economic Commission for Europe's automotive cybersecurity requirements. The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) released regulations (UN R155) stipulating management systems for digital security in passenger vehicles and a legal framework for over-the-air updates, among other controls (Wuhrmann et al., 2023). American manufacturers do not need to comply since the United States is not a member of the UNECE Transportation Agreements and Conventions. Regulators recommend that all brands comply, however, doing so is optional for companies producing vehicles in countries outside of this organization. The EU enforcing this regulation in 2024 demonstrates that governments are only beginning to regulate automotive cybersecurity in vehicles (VicOne, 2023).

Therefore, some governments have internal regulations, others adopt more widespread ones like UN R155, while those like the United States do not regulate their car manufacturers. Considering the current standards, self-regulation practices, and governmental regulations, widespread and enforceable regulation with actionable methodologies does not yet exist. These current frameworks illustrate that regulations in this industry have yet to mature.

REGULATIONS FOR OTHER SECTORS

Considering that current regulations lack standardization, regulations of other sectors illustrate the gaps in the emerging industry of connected vehicles. One such industry that is useful to examine due to its sharing similar problems as the automotive industry is the payment card industry. The Payment Card Industry Data Security Standard sought to standardize cybersecurity regulations for organizations that collect, store, process, or transmit cardholder data. Investigating the timeline of the regulation relative to the industry's growth provides stark comparisons with regulating automotive cybersecurity.

In the early twenty-first century, payment using credit cards began growing to become commonplace today. Before 2004, credit card providers such as Visa, MasterCard, and American Express had individual frameworks for regulating security in transactions with their cards. This initial structure was problematic for businesses since each credit card required a different set of security controls, some of which conflicted. Thus, businesses were limited in what cards they could accept (Seaman, 2020).

To solve this lack of standardization, the Payment Card Industry Security Standards Council introduced the Payment Card Industry Data Security Standard (PCI-DSS), a framework of security controls for handling credit card data. This led to merchants only needing to implement the controls of one framework and being free to accept any credit card protected by PCI-DSS. This regulation was mutually beneficial because credit card companies combine their experience with security controls for an updated framework. Those in compliance with PCI-DSS saved significant resources by

adhering to one framework. The timing of this standard was ideal due to the electronic and online payment sector being in its infancy (Seaman, 2020).

Like the automotive industry, the payment card industry is not unique to one country or world region. Personal vehicles and credit cards are sold and used internationally. Therefore, regulations and standards that cross borders are needed to protect customers around the globe. However, enforcing a global regulation comes with challenges since governments cannot impose such consequences outside of their jurisdiction. A different method of enforcement and consequences is needed if the regulation governs organizations on an international scale.

PCI-DSS is not enforceable by governments, but rather by the credit card companies themselves. Organizations complying with this framework do so by a contractual obligation between the credit card companies with which they conduct transactions. If a merchant breaches such a contract, the credit card companies can impose fines or even prevent transactions with the credit card processor in question. Therefore, PCI-DSS relies on the credit card companies themselves to enforce compliance with the framework to any company accepting their credit cards, regardless of location (Seaman, 2020).

Considering this international scale, how does PCI-DSS interact with regional regulations? The creators did not intend for the framework to replace local, regional, or national laws governing credit card data. Instead, it serves as a list of minimum requirements for protecting cardholder information. The framework seeks to be standardized around the globe and thus does not conflict with existing regulations. Such local laws are seen as an addition to the controls enforced by PCI-DSS. The automotive

industry could follow this approach and rely on corporations for enforcement while allowing regional bodies to impose additional restrictions (Shihab and Misdianti, 2014).

There are many intriguing comparisons between regulating the credit card and automotive cybersecurity industries. As discussed previously, car manufacturers may impose internal regulations on their suppliers just as credit card companies had individual regulations before PCI-DSS standardized them. Similarly, suppliers of digital components for connected vehicles may find difficulty in complying with regulations from different manufacturers as credit card processors did before PCI-DSS. Because of this complexity, both industries require international standardization.

These similarities reveal the gaps between regulating the two industries. PCI-DSS came when electronic payments were still developing. However, connected vehicles are already on the road. Therefore, the first gap is the timeline for regulation. PCI-DSS's introduction during the early development of its industry led to widespread adoption (Seaman, 2020). The automotive industry may have missed this opportunity as countries only recently adopted UN R155. Furthermore, standards like UN R155 are largely optional whereas credit card companies can enforce PCI-DSS through contractual obligations.

However, the automotive industry cannot exactly emulate credit card regulations due to differences between the industries. The supply chain strongly differs between the two sectors. The Payment Card Industry mostly concerns card issuers, payment processors, and merchants whereas the automotive supply chain involves many suppliers from raw materials to dealerships. Widespread regulation in the automotive industry must focus on suppliers more than PCI-DSS. Ultimately, investigating international standards

such as PCI-DSS can inspire regulating automotive cybersecurity on a global scale as long as such a regulation addresses the sector's specific intricacies.

KEY PLAYERS AND STAKEHOLDERS

Several key stakeholders are relevant to automotive cybersecurity: governments, parts suppliers, carmakers, cybersecurity researchers, and consumers. In addition to being key regulatory bodies, governments serve other critical roles as a stakeholder in automotive cybersecurity. The first of which is through funding research and development of information security technologies in connected vehicles. For example, in 2017, the UK Government invested 1.9 billion pounds into a five-year cybersecurity initiative after discovering that cyberattacks in the year prior affected about two-thirds of the country's large businesses (Kim, 2017). This investment's impact went beyond the financial resources themselves. It put the entire country and international partners on high alert regarding cybersecurity issues. Governments taking issues such as automotive cybersecurity strongly enough to commit resources significantly heighten its significance and resulting development.

Governments can also collaborate with the automotive industry to share expertise on thwarting threat actors. By joining forces, the government can help the automotive industry stay updated with the latest cybersecurity threats and security controls. Additionally, the government can play a role in facilitating collaboration by providing a standardized forum for stakeholders to convene and share their knowledge and expertise. If a government investigation into a cyber incident involves connected vehicles, the

agency handling the investigation can include best practices on stopping such attacks in the final report and make it available to the industry. Thus, the government is a key player in automotive cybersecurity whether it be regulation, investment, or collaboration. Its ability to influence the criticality of an issue and enforce best practices is essential to ensure connected vehicles are safe and secure.

Suppliers are the most complex stakeholder in automotive cybersecurity since they provide components for connected vehicles from all around the globe. The number of electronic components and dependencies on software is increasing. Suppliers produce parts with attack surfaces such as electronic control units, infotainment systems, driver assistance systems, and more. They must ensure each subcomponent link is secure to protect the final product. Achieving this goal may be troublesome since different suppliers may produce components that closely interact with each other. Therefore, having strict API rules is essential to ensure no vulnerabilities exist between components of different suppliers. Maintaining the security of their own cyber-systems is also essential to automotive cybersecurity because suppliers may have diagnostic back doors to components in connected vehicles. Therefore, suppliers pose a significant regulatory challenge due to their quantity and geographic dispersal.

Carmakers are the central stakeholders in automotive cybersecurity. Since they ultimately package all the components together to produce a final product for sale to customers, they may be subject to the most regulation in this industry. Some automakers such as Tesla produce their software in-house but still rely on hardware from suppliers. Other automakers may rely more heavily on suppliers for the software within connected vehicles. Nonetheless, they possess the responsibility to ensure their suppliers are

following regulations and conducting the best security practices. This draws a parallel to PCI-DSS. If a merchant outsources payment processing with credit cards to a third party, it has the responsibility to ensure that the third party complies with PCI-DSS. Therefore, automakers are ultimately responsible for the digital security of connected vehicles and complying with relevant regulations.

Cybersecurity researchers and experts provide a critical outside perspective on the issues concerning connected vehicles. Ethical hackers can put vehicle systems to the test as they have significant experience in compromising connected systems and presenting their findings to the system owners. However, most vehicle systems are proprietary and thus closed-source to such penetration testers. Thus, researchers resort to black-box testing, where they have no knowledge of the inner workings of an electronic control unit for example. Grey or white-box testing, where ethical hackers have such information, can be more successful in discovering vulnerabilities. Automakers are beginning to realize the benefits of such security assessments as Ford, Stellantis, General Motors, and Tesla now have bug bounty programs (Hayes, 2020). Automakers can be more open for cybersecurity researchers to test their connected vehicle systems to take full advantage of the value these stakeholders provide. Doing so may also improve the automaker's reputation since it would allow it to be more transparent regarding cybersecurity.

Cybersecurity experts can also help car manufacturers navigate the complexities of legal and regulatory requirements. Individuals versed in both law and information security would be invaluable consultants to a carmaker as the current regulatory landscape widely varies across regions. Automakers may outsource the security assessment of their supplier network to these experts so they can focus on the vehicles

themselves and the customer experience. By collaborating with cybersecurity researchers and experts, automakers can ensure that their vehicles meet legal and regulatory requirements, reduce the risk of cyber threats, and maintain consumer trust in their brand. This can help protect the company's reputation and financial well-being, while also ensuring the safety and security of its consumers and drivers.

The final critical stakeholders are those that use the final product: the consumers and drivers of connected vehicles. An attack on a connected vehicle can compromise a driver's privacy, financial information, and physical safety if the breach can affect the vehicle's movements. Therefore, vehicle owners expect their cars to have defensive measures for these attacks. As they store more information on their cars such as contact details, their home address, payment information for subscription and charging services, and more, they become increasingly trusting of the security controls in their vehicles.

Like governments, manufacturers, and cybersecurity experts, vehicle owners can contribute to improving automotive cybersecurity. Educating end-users is critical to the protection of any device (Zhang-Kennedy and Chiasson, 2021), and connected vehicles are no exception. Consumers have control over critical entry points to their vehicle's systems, such as what network they use for over-the-air software updates. Connecting their vehicle to unknown or open networks poses an opportunity for threat actors to spy on the data being transmitted or inject malware. Vehicles that connect to the owner's smartphone or computer may have an associated account which they must protect via a strong password and two-factor authentication. Any device with the best security measures can still be breached via improperly educated users.

Compromising connected vehicles on a large scale, such as causing gridlock in a congested city, expands the scope of stakeholders to the entire community. Even the safety of road users without connected vehicles may be at risk if such vehicles' movements are maliciously overpowered. Therefore, these four critical stakeholders of automotive security can each contribute to a safer road experience, but individuals outside of these groups are still not immune to such risks.

CHALLENGES

Many challenges arise when proposing standardized regulations for automotive cybersecurity. In addition to the hardware and software of connected vehicles being proprietary to each manufacturer and closed source, today's vehicles have become immensely complex. Electronic control units (ECUs) are computers that control specific components within the vehicle from propulsion to electric seat adjusters. A modern vehicle may have hundreds of these ECUs. Furthermore, these ECUs come from different suppliers and feature designs of different ages (Halder et al., 2020). Diversity in vendors may be viewed as a positive in other aspects of cybersecurity, but combining components made with differing security standards into one product presents significant hardships in regulating the suppliers producing them to the automakers assembling them.

This immense complexity in modern vehicles leads to a dependency on cybersecurity experts within the automotive industry. Security assessors and penetration testers will need to spend a far greater amount of time evaluating the security posture of connected vehicles. Also, over-the-air software updates may open further vulnerabilities

since each ECU may be running different operating systems and different versions of those systems. A single update to a vehicle's software must interface with hundreds of millions of lines of code from a highly varied collection of codebases (Halder et al., 2020). These vehicles have numerous attack surfaces and potentially unsafe and old technology. Regulating cars to minimize these risks must acknowledge this significant challenge and strive to accommodate the intricacies of vehicular networks and vehicles themselves.

To further inhibit security experts evaluating connected vehicles, their embedded technology is rapidly evolving. With such a significant amount of code within one vehicle, automakers must manage and patch the vehicle's software to ensure its safety not only when it is sold new but also during its operational lifespan. As a result of this rapid development, automakers turn toward over-the-air updates, so their customers need not make frequent trips to service centers for manual updates by physically connecting a device to the vehicle (Halder et al., 2020).

Vehicles themselves are also impacted by rapidly evolving technology in the industry. The electrification of passenger vehicles and the development of autonomous driving systems each contribute to more ECUs and lines of code. Electric vehicles offer features such as locating compatible charging stations based on the vehicle's current location and available range and can even handle payment internally rather than at the charging terminal. Autonomous cars look toward vehicle-to-everything networks for information on upcoming traffic lights and the location of other vehicles in their vicinity. These new technologies primarily rely on vehicular networks and developments in software, both of which may increase available attack vectors.

These ways in which technological advancements change the modern automobile significantly contribute to the challenges of regulating automotive cybersecurity. New technology integrating into vehicles may lead to regulations becoming outdated. Complying with outdated regulations may lead to automakers legally selling unsafe vehicles to customers who only see that their car is certified, albeit against obsolete standards. New technologies also lead to new supplier networks with different business models. Existing regulations may not adequately ensure the security of such innovations.

Another challenge with regulating automotive cybersecurity is the different regulatory frameworks across jurisdictions. Different countries require different ways of handling user data, whether it be collected and stored by a connected vehicle or any other device. For example, the European Union's General Data Protection Regulation (GDPR) requires that a company must delete all of an EU citizen's data if they request to be forgotten (Mangini and Moldovan, 2020). The United States however lacks such a regulation. In this case, since vehicles produced in one region may be sold in another, a standardized regulation must be broad enough to accommodate these regulatory differences while being strict enough to properly ensure the customer's digital and physical safety.

Automakers that span multiple jurisdictions, such as those with factories in several world regions, also face immense complexity in creating one design that complies with different regulations. Due to the vastness of supply chains in the automotive industry, any automaker faces the regulatory challenge of enforcing suppliers' compliance with regulations from other countries even if they assemble vehicles in a

single country. Thus, a standardized regulation must also accommodate automakers and supply chains that span multiple regions, each with different regulations.

Enforcing a standardized regulation is also an obstacle because different countries have different legal systems that govern ways in which businesses are held accountable for not complying with widespread regulation. GDPR has enforcement guidelines, but they only apply to organizations handling EU citizen data. If a cybersecurity incident involving connected vehicles occurs in several countries, the legal intricacies of investigating, reporting, and holding parties accountable become complex. Therefore, standardized regulation must globally coordinate such requirements and enforcements.

Considering the stakeholders discussed earlier, these different groups within the automotive industry will have different interests, some of which will conflict. Conflicts of interest present challenges in any regulation. For example, auto manufacturers may prefer inexpensive and fast-to-produce security controls in connected vehicles while governments prefer the best and most costly solutions available when creating regulations. This conflict of interest may lead to automakers lobbying the government to create more favorable regulations. Doing so may harm the overall safety and security of customers of these vehicles.

The customers themselves also share a similar conflict of interest with the automakers. Manufacturers may prioritize profitability and marketability. They may advertise compliance with old standards or mention the modern security controls in some systems while hiding older ones with known vulnerabilities. If the consumer is not knowledgeable of security controls, they may falsely believe that their vehicle is protected from cyberattacks. On the other hand, the consumers ultimately want the maker

of their vehicle to be honest and take effective preventative measures. This conflict of interest creates a tradeoff between profitability and security. Widespread regulation can ensure a baseline level of security controls.

Furthermore, security researchers want the ability to “look under the hood” of digital systems to best evaluate their security posture. However, automakers want to keep their designs proprietary. Even if they use components from suppliers, their integration of such components may be unique. This conflict of interest has significant implications since it may inhibit collaboration in discovering and resolving security vulnerabilities. Good regulation must set out to address these conflicts of interest.

PROPOSED REGULATORY APPROACHES

Is there one best approach to regulating the cyber risk of connected vehicles? The answer to this question is complex. Like other industries, regulators employ different tactics and methods to minimize risk within a specific industry. A more traditional approach is prescriptive regulation. In such a model, regulators set concrete technical and procedural requirements (Barua et al., 2016). The regulated entities receive an exact list of steps or requirements. For example, such a regulation may require the exclusive use of WPA3 encryption for Wi-Fi networks and specifies configuration metrics. Regulators may prefer widespread prescriptive regulation in industries with direct impacts on public health, safety, or the environment. One advantage of this approach is that the regulations are easy to enforce because a regulated entity either meets the specific requirements or does not.

However, this form of regulation's key disadvantage is that it does not leave space for innovation to potentially meet the same outcome more efficiently (Barua et al., 2016).

As mentioned earlier, the technology of automotive cybersecurity itself develops rapidly. Therefore, prescriptive regulation may stifle this innovation. If a stakeholder developed a new, more effective method to secure an aspect of a connected vehicle, they may have to lobby for a regulatory change if the new method does not include the exact steps of prescriptive regulation. Doing so would slow down the development of new technologies and may lead to regulation ultimately discouraging innovation. However, such an approach can be useful in a limited capacity such as enforcing minimum security controls like the availability of key vehicle systems. Prescriptive regulation, although flawed in this context, can still improve security.

Performance-based regulations are a modern alternative to prescriptive regulations. Rather than specifying the exact steps to achieve a risk-minimizing outcome like prescriptive regulations, performance-based regulations focus on the outcome itself. They allow the regulated entity to implement the technical and procedural controls they want to achieve the required outcome (Barua et al., 2016). As an example, a prescriptive regulation over buildings would enforce exact metrics such as materials and wall thicknesses whereas a performance-based regulation would only specify the level of seismic activity that a building must withstand.

A study on offshore drilling regulation compared largely prescriptive regulations in the United States with those from the United Kingdom which are mostly performance-based. They found that initially, there were more incidents under the American prescriptive regulations than the British performance-based ones. The gap has since

closed after a major incident led to more regulation in the United States. In addition to higher incident rates, prescriptive regulations resulted in higher compliance costs and delayed adoption of new safety technologies (Barua et al., 2016). Thus, prescriptive regulations can stifle innovation and increase overhead costs without significantly improving safety when compared to performance-based regulations.

Performance-based regulations may significantly benefit the automotive industry despite not having a drastic effect on incident rates. They create space for the diverse digital systems in vehicles from different manufacturers, a critical element of the industry. Such regulation also allows automakers the freedom to innovate and develop new features and security controls to protect connected vehicles. As cars become more like computers, they become a part of the rapid rate of development in the technology industry. Performance-based regulations give automakers the needed flexibility while prescriptive regulations can enforce minimum requirements to ensure user safety.

Methods of enforcing regulations also exist in several forms. Third-Party certification is a process in which an independent organization evaluates a product or service and its compliance with a given framework. These third parties allow customers and regulators to trust that the commodity meets a desired standard (Tanner, 2000). They provide a critical service of verifying compliance and holding companies accountable for their claims to safety, privacy, and security. This process ultimately creates a level of trust in the marketplace for a product or service among every stakeholder.

For example, as discussed with the PCI-DSS regulation, the regulator relies on regulated entities and third parties to verify that a merchant safely handles a customer's payment information. Credit card companies may enforce the regulation themselves as

per their contract with a merchant or hire an independent third party to conduct the assessment (Seaman, 2020). Both methods lead to an outside organization verifying compliance rather than the merchant merely claiming to do so.

Applying third-party certification to the automotive cybersecurity space involves several steps but would result in greater transparency in the safety of connected vehicles. First, the regulatory bodies must certify the third-party organizations themselves as trusted entities to evaluate automakers. These organizations must be fully independent without any conflicts of interest. Then, these organizations must certify vehicles for sale against a regulation before it is released to ensure the vehicle is safe in its current state. Due to evolving technology, regulators need to implement a process for ongoing compliance checks so that its owner's safety and privacy continue as automakers update the software on the vehicle. Third parties with no direct interest in the automotive industry help automakers stay honest and improve their reputation.

Public-private partnerships can provide a mutually beneficial approach to regulating automotive cybersecurity. By combining the interest and expertise of the two sectors, such partnerships can produce regulations and enforcement approaches that will best address the many complexities of hardening connected vehicles. Partnerships can also better facilitate the exchange of information among all stakeholders involved. Data on the latest threats and mitigations can benefit automakers, governments, and regulatory bodies that look after overall consumer safety. These partnerships will enable connected vehicles' prevalence by ensuring they remain safe over long periods.

If public and private entities collaborate on producing a regulation, they can strike the ideal balance between a regulation's many parameters. Without these relationships,

private industry may prefer performance-based internal regulations that allow freedom in innovation whereas governments and regulators may prefer a prescriptive-based approach because such regulations are relatively simple to enforce. By partnering to form a widespread regulation, the two groups may decide on a hybrid approach between performance and prescriptive-based regulation that balances the ease of enforcement while not stifling innovation (Spraul and Thaler, 2019).

By combining these sets of expertise, public-private partnerships could create synergies beyond developing regulations themselves. Funding for research and development may increase with cybersecurity grants from public bodies and the skills of engineers in private organizations. Such an approach to development can lead to cutting-edge technologies that are not proprietary to one company. Therefore, public-private partnerships can massively contribute to regulating this industry by striking a balance between different stakeholder interests.

CASE STUDIES

The North American automotive industry provides unique insights into the differences in regulating automotive cybersecurity over different continents. Particularly, new domestic entrants, namely Tesla, expose how the domestic industry reacts to disruptive technologies. The industry itself is notably slow to move with only a few players. Three U.S. automakers, General Motors, Ford, and Chrysler accounted for nearly half of the U.S. car industry's market share. As a result, new entrants into the industry face

monumental barriers. Before Tesla, no new domestic brands entered the market on a significant scale since the 1920s (Sull and Reavis, 2019).

Tesla broke this trend by quickly building brand loyalty through unprecedented innovation. Their powertrains, delivery model, maintenance, and more were all in stark contrast with legacy automakers' business models. Since Tesla's entrance, these legacy manufacturers have begun to adopt similar innovations. This disruption to the market clearly illustrates the American automotive industry's slow willingness to innovate unless it is imperative to do so (Sull and Reavis, 2019).

Developing novel technologies like over-the-air updates and autonomous driving also exposes the slow rate of regulation. Tesla noted that the biggest challenge in autonomous vehicles is regulatory approval. Furthermore, less than ten percent of the largest American cities included language regarding autonomous vehicles in their laws and regulations (Sull and Reavis, 2019). This trend also holds for regulating automotive cybersecurity as there is little enforceable regulation on the topic (NHTSA, 2021) and American manufacturers need not comply with otherwise widespread regulation from the United Nations (VicOne, 2023).

Discussing the rate of change in the European Union's automotive industry also provides an interesting case study of European car regulations. As per the Paris Agreement, the EU must reach zero carbon dioxide emissions by 2050. Since nearly half of the transport sector's twenty-seven percent of such emissions are attributable to passenger vehicles in Europe, the industry must change. Yet, despite the immense pressure in the wake of the Volkswagen emissions scandal, automakers remain resistant to such change (Pichler et al., 2021).

An empirical study by Pichler and colleagues (2021) assessed whether European industrial policy encourages or discourages industry from transforming to a more sustainable future. It noted that industrial policy in Europe currently incentivizes external competition with cars produced in different world regions. Therefore, it promotes innovation with the intent to improve economic growth rather than achieve social and environmental goals (Pichler et al., 2021). This policy contrasts with the North American case study since regulators in Europe were faster to drive change in the industry but pushed the transformation in a direction contrary to their ultimate desired outcome.

Considering that European automakers, like North American ones, were resistant to change, they ultimately moved but for different reasons: a new entrant in North American Markets and regulation in European markets. These observations apply to automotive cybersecurity in the future since North American manufacturers may try to self-regulate through market pressure where European ones may do so through government regulation. However, unlike the U.S., the EU will adopt more widespread regulations in this sector from the United Nations (VicOne, 2023). Ultimately, the EU can drive change but has done so in the past with different intentions than the end goal.

In looking at automotive industries in Asia, one must consider the Japanese and South Korean markets as their vehicles and designs are seen throughout the globe. The largest manufacturer by volume, Toyota, was delayed in adapting to industry trends, particularly regarding electric vehicles (Sull and Reavis, 2019). However, like the EU, Japan and South Korea will adopt the UN R155 regulation to stay vigilant on cyber threats to connected vehicles.

Chinese automakers currently impact the global automotive industry and are expected to grow further in their influence. As their government opens state-owned manufacturers to the world and leaves room for startups, technologies from China are integrating into cars made in other world regions (Teece, 2019). Although not widespread yet, the Chinese government desires its automotive industry to become fully entangled with multinational firms while imposing economic disadvantages on foreign players which have experienced significant revenues in the Chinese market. Nonetheless, the rate of change in this market is unique since many of the automakers are in their infancy in a world moving toward connected and autonomous vehicles. The Chinese government used multinational partnerships in the past to collect technology for application in Chinese-made vehicles (Teece, 2019). A future question is when these roles will reverse.

Regulating Asian markets may differ between Japanese and South Korean automakers versus Chinese automakers. Japan and South Korea are clear in their adoption of UN R155. However, Chinese automakers are less established and operate under more forward-thinking policies than the other markets (Teece, 2019). Furthermore, China's non-transparent state capitalism will present difficulties in establishing widespread regulation as it sells more cars to outside countries.

RECOMMENDATIONS

Based on the research in this study, it is recommended that regulators foster collaboration among stakeholders, continuous monitoring, transparency, and consumer awareness. When creating widespread regulation for automotive cybersecurity, a key

recommendation is doing so with collaboration among stakeholders. Automakers, governments, security researchers, and consumers all have differences in their perspectives on the security of connected vehicles. A standardized regulation must accommodate these different interests to be widely accepted. Such collaboration will ensure each voice is heard so the regulation reflects the market as a whole rather than one group's desired outcomes.

Furthermore, collaborating on new regulations may increase the legitimacy among the different parties. If each stakeholder can claim part ownership of the policy, it will be significantly easier to achieve buy-in across continents. This sense of ownership can create widespread support for the regulation, reduce opposition and improve the rate and enforcement of compliance. Reducing conflict in regulation poses numerous benefits. By establishing common ground, each stakeholder may be more willing to make compromises, thus fostering smooth implementation.

As seen in the European Union's industrial policies, the regulator's end goal may differ from the original intention of regulation. By collaborating with stakeholders, each party can help ensure the regulation's effectiveness in achieving the desired outcome, which is protecting the safety, security, and privacy of the drivers of connected vehicles. For example, regulators can learn from industry experts about topics such as new technologies that may conflict with a proposed requirement in the future. Collaboration among stakeholders fosters effective regulations that address all parties involved.

Including regulation that requires automakers to continuously monitor and safely update connected vehicles is a key recommendation due to being a unique security concern. Most personal devices such as smartphones and computers do not reach the

average age of a car in the United States. Therefore, as cars incorporate the ability to connect to the internet, updating them to ensure safety over their useful life is critical (Bécsi et. al, 2015). Since over-the-air updates, particularly those that affect vehicle control systems, present a significant attack surface, regulations must be stringent in ensuring that automakers release such updates, but do so safely.

The need for continuous monitoring and updating also applies to automotive cybersecurity regulations themselves. The threat landscape in any industry is extremely dynamic as new security controls are implemented and threat actors find new exploits. Considering these rapidly changing cyber threats, regulations must keep pace. Collaborating with all stakeholders enables such updates to regulation since security researchers can notify automakers and governments of new threats that may be addressed with new regulations. Novel technology also contributes to new threats unforeseen by regulators. For example, software that may be updated over the internet is increasingly in control of a vehicle's movements with autonomous technology. In this case, new regulations may be needed to further inhibit malware's ability to affect these systems. Therefore, with the rate of change in the threat landscape and new technology in connected vehicles, regulators must have the ability to quickly update policies.

Such regulation also requires continuous monitoring of compliance. Automakers may initially meet a regulation's requirements but may not with new vehicles in the future. Noncompliance must also be quickly identified and addressed.

Another recommendation in automotive cybersecurity is enforcing transparency among regulated entities. Car companies often prefer to keep any reliability issue with one of their vehicles out of the public eye until a fix is ready. They may also want to

retain all the details surrounding proprietary technology to maintain competitive advantages. Although consumers tend to freely switch between brands without high loyalty (Sull and Reavis, 2019), car companies still desire to maintain a reputation of reliability without rivals looking under the bodywork. These desires present a strong gap that regulation must address since transparency in revealing cyber incidents is critical.

Transparency among automakers will ensure that they are all complying with cybersecurity regulations. Enforcing a regulation across several continents poses significant challenges due to different governing bodies. Automakers concealing the security controls in their vehicles would hugely exaggerate such challenges. Furthermore, as cyber law concerning reporting breaches may change in the future, automakers may be required to publicly disclose cyber events. Transparency in these instances of failure is critical for regulators and security researchers to prevent such an occurrence in the future. This streamlined communication is imperative in cybersecurity because the threat landscapes can change overnight.

Therefore, holding regulated entities to be transparent and accountable for their actions through regulation will vastly improve the safety, security, and privacy of connected vehicles and their owners without significant costs. Doing so allows those enforcing the regulation to easily assess a carmaker's compliance and overall security posture. Collaboration in regulation will ensure that automakers will meet transparency standards without revealing proprietary technology.

The last critical recommendation for regulating the automotive cybersecurity industry is promoting consumer education and awareness. Even if a manufacturer develops a connected vehicle with an adequate security posture, the end user may

compromise their own safety, security, or privacy. A weak password to the account associated with a vehicle and unsafe internet connections for over-the-air updates are some of the reasons why an end-user can increase the threat of malicious actors compromising their vehicle. Thus, enforcing consumer education and awareness is critical to help consumers understand the risks of connected vehicles and encourage them to take appropriate measures to protect themselves and other road users.

Coinciding with the previous recommendation, consumers must be aware of known vulnerabilities and cyberattacks that may affect their vehicle. If automakers are transparent with this information, their consumers can be more pertinent to a breach. Educating consumers on how to identify a breach, such as unexpected behavior from the vehicle or changes to their account, is also important so they can take immediate action to quarantine the vehicle before the damages become worse. Otherwise, they would need support services which could lose those crucial first few minutes in a cyber incident.

Lastly, consumers must be made aware of the shared responsibility model with their product. The automaker would be responsible for building a secure vehicle and for continuous monitoring and updating whereas the consumer must harden their side of the product, such as the account and devices used to access vehicle systems. They also have the responsibility to be transparent with the automakers to notify them of any suspicious activity. Overall, regulation must ensure that consumers are armed with the knowledge to fulfill their responsibility in securing the ecosystem of connected vehicles.

CONCLUSION

Ensuring automotive cybersecurity is a novel challenge as connected vehicles become more commonplace. Today's cars can provide Wi-Fi for the passengers, link with city grid systems, allow remote locking, unlocking, and starting, and much more. These features can make driving a car safer and more convenient. However, such vehicles now connect to the internet in real-time, thus creating an unprecedented attack surface. Threat actors can compromise a driver's privacy through the vehicle's location, stored addresses, and payment information for charging stations and subscription-based features. They can also threaten the driver's physical safety by controlling the vehicle's movements (Ornes, 2020). As mentioned earlier, even those without connected vehicles are at risk as threat actors can cause gridlock in dense cities. New technology with this level of impact must be regulated to ensure global safety.

Therefore, how should governments regulate automotive cybersecurity? Firstly, the regulation must be uniform across the globe due to suppliers and assemblers located worldwide. Few of the current regulatory frameworks cross borders and most only rely on national governments for enforcement. Automakers may self-regulate but will do so with different intentions that may put a particular region more at risk than another since new players in the global market, namely in China, strive for internal goals. Other widespread regulations such as the PCI-DSS may serve as a template since it regulates any merchant regardless of location and relies on corporations to enforce the requirements through contracts. Nevertheless, regulating connected vehicles has stark differences from other industries due to the complexity of vehicle systems, rapidly

evolving technology, regionally differing methods of enforcing regulations, and conflict of interest among the key stakeholders. Automakers want to keep proprietary technology private and withhold the freedom to innovate, while governments want transparency and control, security researchers want access to internal systems, and consumers want feature-packed vehicles.

Differing regulatory approaches such as prescriptive and performance-based offer positives and negatives. Regardless, each would rely on third-party certification to minimize conflicts of interest and public-private partnerships to foster mutually beneficial requirements. Considering how the North American, European, and Asian markets develop and respond to change in converse ways, a regulation must accommodate such regional differences. Therefore, the ideal regulation over automotive cybersecurity enforces minimum security controls regardless of where the vehicle or its parts came from and is one that governments enforce on automakers, who enforce on their suppliers. Through a hybrid prescriptive and performance-based regulation, it can enforce key outcome metrics while allowing innovation. This regulation, through stakeholder collaboration, continuous monitoring and updating, transparency, and encouraging consumer education, will enable the future of connected vehicles.

This study focused on the potential problems and challenges of regulating cybersecurity of connected vehicles and did not discuss some of the emerging and future developments in this industry. For example, new approaches to securing connected vehicles such as blockchain for advanced cyber-resilience may revolutionize the threat landscape (Fraga-Lamas and Fernández-Caramés, 2019). Also, risks to modern motoring extend beyond the vehicles themselves to infrastructure such as electric vehicle charging

networks, which attackers have already targeted in the Russian invasion of Ukraine (Pourmirza and Walker, 2021). These future changes and vulnerabilities pose new paths for research.

In conclusion, as the automotive industry relies more heavily on connected technology, governments are only beginning to take steps to regulate automotive cybersecurity. Through initiatives and regulations, the public and private sectors must address the critical need to ensure the safety, privacy, and security of drivers, passengers, and pedestrians by enforcing minimum security controls. While there are still challenges to overcome, such as balancing privacy concerns and cybersecurity needs with the demand for new features, the increasing focus on transparency, accountability, and consumer education is a positive step toward creating a secure and trustworthy automotive ecosystem.

REFERENCES

- Barua, S., Gao, X., & Mannan, M. S. (2016). Comparison of prescriptive and performance-based regulatory regimes in the USA and the UK. *Journal of loss prevention in the process industries*, 44, 764-769.
- Bécsi, T., Aradi, S., & Gáspár, P. (2015, June). Security issues and vulnerabilities in connected car systems. In *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* (pp. 477-482). IEEE.
- Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-depth exploration of ISO/SAE 21434 and its correlations with existing standards. *IEEE Communications Standards Magazine*, 6(1), 84-92.
- Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE access*, 7, 17578-17598.
- Halder, S., Ghosal, A., & Conti, M. (2020). Secure over-the-air software updates in connected vehicles: A survey. *Computer Networks*, 178, 107343.
- Hayes, J. (2020). Hackers under the hood: It's been five years since the first reports of car hacking emerged, but despite progress in vehicle protection standards, automotive cyber-security remains on high alert. *Engineering & Technology*, 15(3), 32-35.
- Hugot, V., Jousse, A., Toinard, C., & Venelle, B. (2019, November). oMAC: Open model for automotive cybersecurity. In *17th escar Europe: embedded security in cars (Konferenzveröffentlichung)*.
- International Standards Organization (ISO). (2021, February 16). About Us. ISO. Retrieved March 10, 2023, from <https://www.iso.org/about-us.html>
- Kim, J. (2017). Cyber-security in government: reducing the risk. *Computer Fraud & Security*, 2017(7), 8-11.
- Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected vehicles: Solutions and challenges. *IEEE internet of things journal*, 1(4), 289-299.
- Mangini, V., Tal, I., & Moldovan, A. N. (2020, August). An empirical study on the impact of GDPR and right to be forgotten-organisations and users perspective. In *Proceedings of the 15th international conference on availability, reliability and security* (pp. 1-9).

- Ornes, S. (2020). How to hack a self-driving car. *Physics World*, 33(8), 37.
- Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE transactions on intelligent transportation systems*, 18(11), 2898-2915.
- Pichler, M., Krenmayr, N., Schneider, E., & Brand, U. (2021). EU industrial policy: Between modernization and transformation of the automotive industry. *Environmental Innovation and Societal Transitions*, 38, 140-152.
- Pourmirza, Z., & Walker, S. (2021, August). Electric vehicle charging station: cyber security challenges and perspective. In *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)* (pp. 111-116). IEEE.
- Seaman, J. (2020). *PCI DSS: An integrated data security standard guide*. Apress.
- Shihab, M. R., & Misdianti, F. (2014, October). Moving towards PCI DSS 3.0 compliance: a case study of credit card data security audit in an online payment company. In *2014 International Conference on Advanced Computer Science and Information System* (pp. 151-156). IEEE.
- Society of Automobile Engineers (SAE). (n.d.). The mission of SAE International is to advance mobility knowledge and solutions. SAE International. Retrieved March 10, 2023, from <https://www.sae.org/>
- Spraul, K., & Thaler, J. (2020). Partnering for good? An analysis of how to achieve sustainability-related outcomes in public–private partnerships. *Business Research*, 13(2), 485-511.
- Strobl, S., Hofbauer, D., Schmittner, C., Maksuti, S., Tauber, M., & Delsing, J. (2018, May). Connected cars—Threats, vulnerabilities and their impact. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)* (pp. 375-380). IEEE.
- Sull, D., & Reavis, C. (2019). Tesla's Entry into the US Auto Industry.
- Tanner, B. (2000). Independent assessment by third-party certification bodies. *Food control*, 11(5), 415-417.
- Teece, D. J. (2019). China and the reshaping of the auto industry: A dynamic capabilities perspective. *Management and Organization Review*, 15(1), 177-199.
- Trovao, J. P. (2020). Automotive electronics under the COVID-19 shadow [Automotive Electronics]. *IEEE Vehicular Technology Magazine*, 15(3), 101-108.

- U.S. National Highway Traffic Safety Administration (NHTSA). (2021, February 2). U.S. National Highway Traffic Safety Administration releases update to Automotive Cyber Security Best Practices. IEEE Innovation at Work. Retrieved March 10, 2023, from <https://innovationatwork.ieee.org/u-s-national-highway-traffic-safety-administration-releases-update-to-automotive-cyber-security-best-practices/#top>
- VicOne. (n.d.). UN R155. VicOne. Retrieved March 10, 2023, from <https://vicone.com/why-vicone/un-r155#:~:text=UN%20R155%20applies%20to%20the%2054%20member%20countries%20of%20the,%2C%20Japan%2C%20and%20South%20Korea>
- Vivek, S., Yanni, D., Yunker, P. J., & Silverberg, J. L. (2019). Cyberphysical risks of hacked internet-connected vehicles. *Physical Review E*, 100(1), 012316.
- Wuhrmann, D., Setfan Hessel, & Deeg, T. (2023, January 31). New UN regulations for cybersecurity and software updates in the automotive industry. Reuschlaw. Retrieved March 10, 2023, from <https://www.reuschlaw.de/en/news/new-un-regulations-for-cybersecurity-and-software-updates-in-the-automotive-industry/>
- Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, 54(1), 1-39.

Name of Candidate: Alex Hewitson

Date of Submission: May 2, 2023