VicOne

Driving Automotive Cybersecurity Forward

Insuring the Future of Mobility:

New challenges for the auto insurance industry and the critical role of automotive cybersecurity

Salvatore Gariuolo, Rainer Vosseler
FTR Research for VicOne

Trend Research for VicOne

Executive Summary

The mobility landscape is on the verge of a fundamental shift. Emerging trends, such as shared mobility, autonomous driving, and vehicle connectivity, are poised to offer new transport options, enhance road safety, and improve the overall driving experience. While these developments provide significant benefits, they will also lead to profound changes in the auto insurance industry. Accidents will no longer be caused solely by human error, but might also stem from software failures or cyberattacks. As a result, the role of auto insurance will evolve, not only protecting individual drivers but also covering car manufacturers (OEMs) against the technological risks associated with their vehicles.

The impact of this shift is substantial as it disrupts the conventional practices auto insurers use to set policy premiums and determine accident liability. Insurers have traditionally relied on claims history and, more recently, on usage-based insurance (UBI), both of which provide data on driving behavior. But with the emerging mobility trends, relying only on driver data is no longer sufficient. The new risks are largely technology-driven, and responsibility may no longer lie solely with the driver. Auto insurers must now develop a thorough understanding of connected vehicle technologies to accurately profile the new risks, as well as gain access to vehicle data to analyse the increasingly complex liability scenarios.

The growing need for technological expertise and vehicle data is set to reshape the dynamics of the auto insurance market. Insurers are likely joining forces with OEMs to improve the accuracy of their premiums and refine liability assessments. However, both groups lack a full understanding of the risks tied to new vehicle technologies, revealing a critical skills gap that automotive cybersecurity companies can help fill. Indeed, automotive cybersecurity can enable insurers to identify the actual and emerging risks connected vehicles face, helping them accurately price their policies. It can also provide auto insurers with insights into what happens during vehicular accidents, allowing them to avoid litigation over liability and reduce claim costs.

In this new mobility ecosystem, VicOne, a leader in automotive cybersecurity, is the ideal partner, bridging the skills gap that even collaboration between insurance companies and OEMs cannot fully address. VicOne's comprehensive solutions help auto insurers better understand emerging vehicle risks and liabilities, enabling them to secure their long-term financial viability.

Table of Contents

Introduction

Auto insurance policies are designed to provide financial protection in the event of an accident. By making regular payments, the policyholder receives coverage for various types of losses, including damage to their vehicle and other property, as well as injuries to the driver, passengers, and other road users. The cost of this protection, known as the premium, is calculated based on the perceived risks associated with the driver, using historical data that allows insurers to estimate the probability and average cost of claims accurately. This approach ensures that auto insurers are able to pay out claims, cover operational costs, and maintain profitability. However, new mobility models and advances in connected vehicle technology are poised to disrupt significantly the way auto insurance operates.

Emerging mobility trends are set to revolutionise the auto insurance industry. In a future dominated by shared and autonomous vehicles, the traditional liability model, where at least one driver is held at fault, may no longer apply. Liability scenarios will be more complex, with responsibility for accidents potentially shared among drivers, technology providers, and even cybercriminals. These new technologies could also introduce unprecedented risks for which no historical data exists, making it difficult for insurers to determine premiums accurately, undermining their financial viability.

To navigate this complex and rapidly evolving landscape, insurance companies should forge strategic partnerships with automotive cybersecurity firms. Automotive cybersecurity experts can help auto insurers better profile the new risk pool, an essential step in setting accurate premiums. They can also assist insurance companies in analysing vehicle data to determine liability for accidents, enabling faster claims resolution, and lower associated costs. Car OEMs and mobility service providers also stand to benefit. By implementing measures to monitor, prevent, detect, and respond to cyber threats around the clock, they can significantly reduce their insurance costs.

Automotive cybersecurity thus serves a dual purpose: it helps the stakeholders in the auto insurance industry remain profitable while also ensuring the safety of all road users in this new era of technological advancement.

Research Objectives

This research examines the increasing importance of automotive cybersecurity in the auto insurance industry, driven by emerging mobility trends. It specifically explores how VicOne can support auto insurance companies in adapting their practices to this evolving landscape. Integrating automotive cybersecurity into traditional insurance practices will be essential for auto insurers to safeguard their profitability amid these new technological risks.

This research is organized into three chapters, each focusing on a key aspect of the study:

> **Chapter 1** provides an overview of emerging mobility trends and their expected impact on auto insurance practices. It explains how these trends will introduce major challenges to insurers by disrupting their traditional approaches to risk assessment and liability determination.
>
> **Chapter 2** examines why these challenges threaten the financial viability of auto insurers. It discusses the need for insurance companies to understand the risks posed by new connected vehicle technologies and to gain access to vehicle data, both of which are essential for adapting their practices and maintaining profitability.
>
> **Chapter 3** emphasizes how automotive cybersecurity can help insurance companies remain profitable amid the evolving mobility landscape. It details how VicOne's solutions can assist insurers in identifying vulnerabilities and potential cyber threats, enhancing their ability to profile risks and determine accident liability.

1. The Auto Insurance Revolution

How emerging mobility trends are redefining the industry

For decades, the auto insurance industry has focused primarily on individual motorists, offering financial protection in the event of a road accident. These policies, known as personal auto insurance, cover a range of losses, including vehicle and property damage, medical expenses for injuries sustained by the policyholder and other involved, and legal costs resulting from lawsuits. These policies can also be extended to cover vehicle theft and damage caused by events other than collisions, such as severe weather or natural disasters.

Today, personal auto insurance represents the largest segment of the auto insurance market [1], reflecting society's reliance on private cars. Historically, cars have given individuals the autonomy to travel on their schedules and routes, offering convenience and a sense of safety unmatched by other forms of transport. This has made the car not only a means of transport but also a symbol of social status and personal freedom. As a result, and amplified by the global population boom, the number of cars worldwide has surged [2], from about 70 million in 1950 to over 1.5 billion in 2020 [3], leading to a corresponding increase in personal auto insurance policies.

However, the auto insurance industry is on the verge of significant transformation. Shared mobility models – such as car-sharing and ride-hailing services – are rapidly gaining traction as sustainable and cost-effective alternatives to traditional car ownership, reducing the demand for private cars and personal auto insurance. At the same time, the rise of autonomous driving is set to revolutionise the concept of liability for road accidents, shifting the responsibility from drivers to car manufacturers and software developers. Alongside these changes, the increasing vehicle connectivity is introducing new risks, such as automotive cybersecurity threats and data breaches, which are not yet adequately addressed by traditional insurance policies.

1.1 Shared Mobility Models

A progressive shift towards commercial auto insurance

The rapid rise of shared mobility is reshaping not only urban transport but also the auto insurance landscape. As more private vehicles are used for commercial purposes through car-sharing and ride-hailing services, insurers are likely to see a shift from personal to commercial auto insurance policies. The profile of policyholders will also change, from individual motorists to shared mobility providers. This shift presents significant challenges, including determining liability in accidents involving vehicles shared by multiple users and assessing novel risks with limited driver data and limited understanding of the new technologies.

Shared mobility is a broad term encompassing various transport options, such as ride-hailing, car-sharing, and micro-mobility, which individuals can access on demand. These services operate via digital platforms, typically through mobile apps that allow users to search, book, and pay for the option that best suits their itinerary and budget. This model has the potential to revolutionise urban transport, as it expands the mobility mix, addresses diverse needs, and simplifies door-to-door trips. Its rapid adoption confirms this potential: shared mobility is projected to account for 7% of all urban journeys by 2030 [4].

Shared mobility models are rapidly gaining popularity as they offer the flexibility of personal vehicles without the financial burdens of ownership [5]. This is particularly evident in large urban centres, where costs such as insurance, parking, fuel, and maintenance are increasingly prohibitive [6]. Their adoption is also driven by a cultural shift, particularly among younger demographics [5]. While cars have traditionally been considered status symbols and markers of personal success, Millennials and Generation Z are less likely to share this view. Instead, they prioritize flexible mobility solutions over the long-term commitment of owning a vehicle [7].

Nevertheless, shared mobility models will not take the same form in every city [8]. Cities with efficient and extensive public transport networks, along with safe and convenient infrastructure for cycling and walking, create an ideal environment for car-sharing and micro-mobility, which are expected to complement public transport. In such scenarios, shared cars can extend access to locations beyond the reach of public transport, while free-floating bicycles and scooters offer convenient last-mile solutions. With their robust public transport systems and policies aimed at reducing car use, European and Chinese cities exemplify this approach. In contrast, areas with limited public transport, such as many in the United States and South America, tend to rely on ride-hailing services like Uber, which often substitute for public transit rather than complement it.

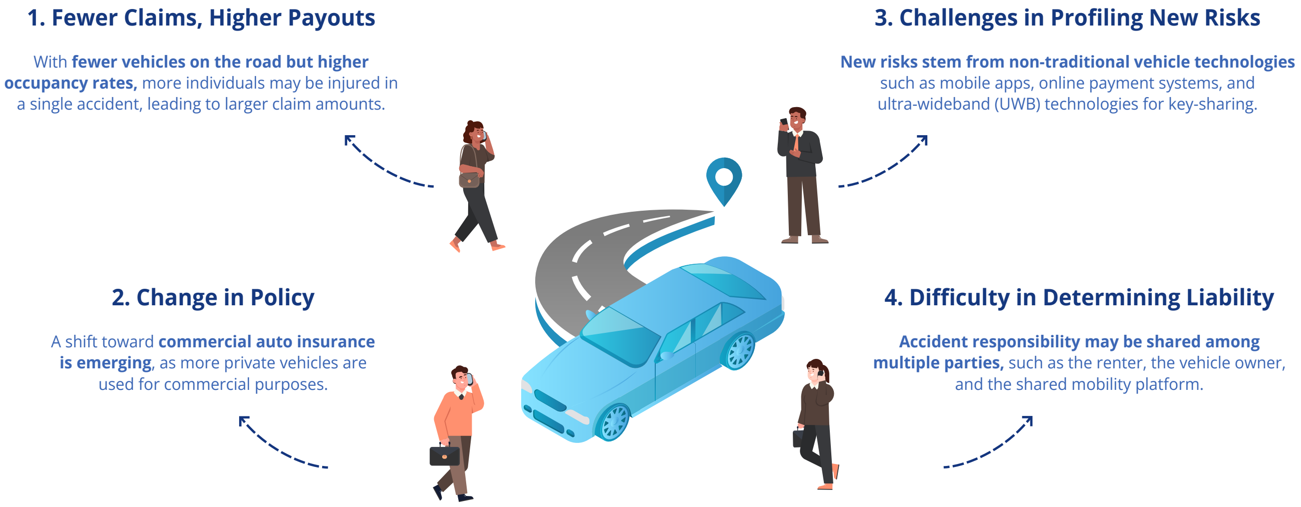
While the type of shared mobility model may vary across regions, the overall impact will essentially be the same: reducing the number of private vehicles. Studies suggest that shared mobility could replace between 9 and 13 private cars [9] – a number that may be even higher in urban areas where this paradigm is widely adopted. This shift will likely reduce demand for personal auto insurance but increase the need for **commercial auto insurance** [10], as more private vehicles are repurposed for business use.

The shift towards shared mobility is also changing the profile of the policyholder: service providers, rather than individual motorists, will be required to underwrite policies for their cars. This applies to ride-hailing services, such as Uber and Lyft, which offer policies that activate during active trips, and car-sharing services like Lynk&Co, which bundle commercial coverage into rental agreements. Shared mobility will also affect the nature of claims. While the total number of accidents is set to decline due to fewer cars on the road [11], each incident may involve more people [12], since shared vehicles typically carry more passengers than private cars. As a result, insurers may face a **lower number of claims, but with greater severity.**

Like personal auto insurance, commercial auto insurance is designed to cover a range of risks related to vehicle accidents, damage, and driving behavior. However, in shared mobility models, **determining liability** for accidents becomes especially complex. Responsibilities may be distributed among several parties, each potentially bearing a share of the liability [13]: the renter, whose driving behavior may have caused the accident; the vehicle owner, who may be at fault for poor car maintenance; and the mobility platform, which could be liable for allowing the vehicle on its platform without adequate checks.

Commercial auto insurance also faces higher risks than personal auto insurance. In models like car-sharing, a single vehicle is used by multiple drivers, some of whom may have limited experience, leading to greater variability in driving behavior and increased associated risks. **Profiling these risks** poses a major challenge for insurers, especially exacerbated by the lack of historical data on individual drivers, which has always been a cornerstone of traditional risk assessment practices [6].

Moreover, shared mobility introduces **novel threats** not typically associated with traditional vehicles. For example, shared cars often use ultra-wideband (UWB) technology for key sharing [14], which, while more secure than key fobs, is not immune to risk. These technology-related threats are more likely to fall under cyber liability insurance, which can help mobility service providers manage the risks linked to cyber threats and data breaches.



1. Fewer Claims, Higher Payouts

With **fewer vehicles on the road but higher occupancy rates,** more individuals may be injured in a single accident, leading to larger claim amounts.

3. Challenges in Profiling New Risks

New risks stem from non-traditional vehicle technologies such as mobile apps, online payment systems, and ultra-wideband (UWB) technologies for key-sharing.

2. Change in Policy

A shift toward **commercial auto insurance is emerging**, as more private vehicles are used for commercial purposes.

4. Difficulty in Determining Liability

Accident responsibility may be shared among multiple parties, such as the renter, the vehicle owner, and the shared mobility platform.

Figure 1.1 Effects of shared mobility on auto insurance

1.2 Autonomous Driving

A progressive shift towards commercial auto insurance

The rise of autonomous driving is transforming the auto insurance industry by gradually shifting responsibility from drivers to vehicles as automation levels increases. As a result, product liability insurance becomes increasingly important, with coverage focusing more on vehicle manufacturers than individual motorists. Insurers will also face new challenges, such as assessing the risks associated with AV technology without fully understanding its complexities, and determining liability in accidents involving both autonomous driving systems and human behaviour.

Autonomous vehicles (AVs), also known as self-driving or driverless cars, are designed to sense their environment and navigate without human input. They rely on a combination of sensors, including cameras, LiDAR, and radar, to perceive their surroundings. Using computer vision and artificial intelligence, AVs process this data to make driving decisions and control vehicle functions such as steering, speed, acceleration, and braking.

Although terms like “self-driving” and “autonomous” are commonly used, no vehicle currently on the market can operate without human supervision. In reality, today’s vehicles require varying levels of human oversight, depending on their designed level of autonomy. To clarify these distinctions, the Society of Automotive Engineers (SAE) developed a classification system that defines increasing levels of driving automation [15], ranging from Level 0 to Level 5.

Level 0 refers to no automation: while the vehicle may provide warnings or momentary intervention systems such as Emergency Brake Assist (EBA), all driving tasks are performed by the human driver. In **Level 1**, the driver remains responsible for most tasks, but the vehicle is equipped with a single advanced driver assistance system (ADAS), such as cruise control or lane keeping assist. At **Level 2**, driving is partially automated, with two or more functions such as acceleration, braking, or steering handled by the vehicle. However, the human driver is still fully responsible for the vehicle’s overall operation.

As the levels progress, there is a shift from systems that assist the driver to those capable of independently handling a wide range of driving tasks. At **Level 3**, the vehicle can drive autonomously under specific conditions, such as on highways or in urban areas where the infrastructure supports it, in clear weather, and under normal traffic conditions. However, the driver must remain available to take control when prompted. At **Level 4**, the vehicle no longer requires human supervision within those predefined scenarios. **Level 5** represents full automation, where the vehicle can perform all driving tasks, with no need for human intervention.

Despite ambitious claims from car OEMs, fully autonomous vehicles are still several years away from widespread adoption. While most manufacturers have achieved Level 2 autonomy – seen in systems like Tesla's Autopilot, Audi's Traffic Jam Assist, and GM's Super Cruise – only 3% of the global car fleet is expected to reach Level 3 by 2035 [16]. High levels of automation are currently limited to the ride-hailing sector [16], with autonomous taxis from Cruise, Waymo, and Baidu operating in cities across the US, China, the Middle East, and now Europe. However, full autonomy remains elusive: reports indicate that Cruise taxis, for example, require remote assistance 2 to 4% of the time [17], suggesting the need for continued human supervision.

Despite the current limitations, autonomous driving offers a major advantage, particularly at higher levels of automation: improving road safety. AVs can detect and respond to incoming hazards with a level of precision that human drivers cannot consistently achieve [18]. Given that human error accounts for approximately 94% of road collisions [19], as reported by the National Highway Traffic Safety Administration (NHTSA), fully autonomous vehicles present a promising opportunity to drastically reduce road accidents. AV technology is also expected to decrease their severity significantly [6] by optimizing the vehicle's emergency responses, such as braking and maneuvering, which can help mitigate the impact of unavoidable collisions. As a result, insurance companies may see **fewer claims** overall. However, those accidents that do occur are likely to involve **higher payouts**, as repairing an AV can cost nearly twice as much as repairing a conventional vehicle.

As discussed, the concept of driver error is expected to diminish with autonomous driving. However, road accidents will not disappear entirely, as faulty sensors, software bugs, or inaccurate GPS data may still cause them. As connected vehicle technology becomes more complex, the likelihood of technical errors also increases. This shift has significant implications for the insurance industry: as automation advances, liability for accidents will move from drivers to vehicles. As a result, the **product liability policy**, which covers the manufacturer's responsibility for defects, will become the primary form of coverage in the event of a collision [20]. Meanwhile, the role of personal auto insurance will also evolve to focus more on liabilities related to vehicle maintenance and misuse, rather than driving errors.

This shift in liability poses significant challenges for auto insurers when it comes to **risk profiling**. Traditionally, insurers based their risk assessments on human behavior, using factors such as driving history, age, and location. With AVs, these factors become less relevant as responsibility for driving tasks shifts to the vehicle's technology. Insurers must now account for risks related to faulty hardware, outdated software [21], and the overall reliability of AV systems. For example, AVs remain vulnerable to collisions with animals due to limitations in sensing technology [22], which can struggle to detect small or fast-moving objects, especially in low light or at high speeds. Therefore, a solid understanding of AV technologies is critical for auto insurers to accurately assess the likelihood and severity of these emerging risks.

Determining liability in accidents involving AVs will also become considerably more complex. Road accidents could stem from multiple sources [23]: the actions or inactions of the human driver, failures in any component of the AV, or issues with the surrounding infrastructure, such as the road itself. Even with fully autonomous vehicles, humans may still be held liable for road accidents [24] – for example, if they tamper with the vehicle or fail to perform proper maintenance. This multi-faceted nature of liability, coupled with the high level of technological complexity of AVs, will make it extremely difficult for auto insurers to determine who or what is at fault. This represents a major challenge, as it affects the insurers' ability to determine how liability is distributed between the two insurances – personal auto and product liability – and how each contributes to covering the resulting damages.

Another growing concern for auto insurers is the digital infrastructure that AVs depend on, which makes them susceptible to cyberattacks. Threat actors could compromise AV operation by spoofing Global Navigation Satellite System (GNSS) signals [25] or interfering with radar and LiDAR systems [26]. There is the potential risk for remote hijacking, where cybercriminals take control of the AV or its components, such as cameras, or even hold it ransom by locking its systems [27]. These **new risks** are not typically covered by traditional product liability insurance, which focuses on manufacturing defects. Instead, they fall within the scope of cyber liability insurance, which is better suited to address the evolving risks tied to vehicle connectivity and software vulnerabilities.

1. Fewer Claims, Higher Payouts

Fewer road collisions but higher repair costs due to the complexity and expense of AV technology.

2. Change in Policy

Shift toward **product liability insurance** as responsibility moves from drivers to vehicle manufacturers.

3. Challenges in Profiling New Risks

New risks stem from non-conventional technologies, such as ADAS and AV sensors, including cameras, radar, and LiDAR.

4. Difficulty in Determining Liability

Road accidents may result from AV malfunctions or the actions or inactions of the human driver.

Figure 1.2 Effects of autonomous driving on auto insurance

1.3 Vehicle Connectivity

A growing risk pool for cyber liability insurance

Vehicle connectivity has transformed the way we interact with our vehicles, transforming them into dynamic, data-driven machines that seamlessly integrate with our digital lives [28]. The rise of connected technologies has enabled new levels of convenience, safety, and entertainment, making driving more efficient and enjoyable. Drivers can now access information, control vehicle functions, and receive real-time alerts while on the move, blurring the lines between the vehicle and the connected world.

At its core, vehicle connectivity involves the exchange of data between in-vehicle systems and external networks or devices. This includes communication with smartphones, wearable devices, and other vehicles, and cloud-based services such as navigation, entertainment, and vehicle diagnostics. As a result, drivers benefit from features such as voice-activated controls, real-time traffic updates, and predictive maintenance alerts – all while maintaining a secure and reliable connection to the vehicle's systems. The impact of connectivity is far-reaching, with implications for safety, convenience, and the overall driving experience.

Cyber liability insurance refers to a type of insurance coverage that protects businesses and organizations from financial losses resulting from cyber-related attacks, data breaches, and other technology-driven threats [29]. As the reliance on digital technologies increases, so does the risk of cyberattacks that can expose sensitive information, disrupt business operations, and result in significant financial losses. In the context of shared mobility and autonomous vehicles, cyber liability insurance is essential for mitigating these emerging risks.

The difficulty in **profiling the risk** of technology-related and cyber threats lies in their novelty and lack of historical data [6]. Unlike traditional risks such as traffic accidents or natural disasters, which are supported by established actuarial models and statistical records, cyber threats are relatively new and unpredictable. This makes it challenging for insurers to accurately assess and price these risks, leading to uncertainty and potential underinsurance in the event of a major cyber incident. **Determining liability** is also difficult, as accidents may result from either driver error or a mere consequence of a cyberattack.

The overlap between shared mobility, AVs, and cyber liability insurance is becoming increasingly relevant as more vehicles connect to the internet and rely on digital systems to operate safely and efficiently. Cyberattacks can compromise vehicle software, data, and communication networks, putting passengers, drivers, and other road users at risk. As a result, the automotive industry is beginning to recognize the importance of cyber liability insurance in addressing these emerging threats. However, this type of insurance is still not widely used in the automotive sector, leaving many stakeholders vulnerable to the financial consequences of cyber incidents. This calls for urgent action, as the frequency and impact of cyber-attacks continue to grow [30, 31].

Below is a list of risks likely to be covered by cyber liability insurance [32]. This coverage is designed to protect car manufacturers and mobility service providers from losses resulting from cyberattacks targeting vehicle technologies, companion apps, back-end systems, and associated data.

Unauthorized data manipulation poses a serious threat, as malicious actors can modify or delete critical vehicle data, potentially causing system failures, endangering lives, or leading to substantial financial losses. This underscores the need for robust authentication and authorization mechanisms to prevent unauthorized access to sensitive information. Such risks can significantly impact auto insurers. If malicious actors manipulate data related to vehicle performance, location, or other critical information, it can lead to false claims or inflated premiums. Insurers may need to reassess their policies and adjust underwriting processes to account for these emerging vulnerabilities.

Data integrity and authenticity compromise risks arise when malicious actors inject fake or tampered data into vehicle systems, potentially compromising vehicle performance and endangering passenger safety. This highlights the importance of implementing secure communication protocols, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), to ensure the integrity and authenticity of data exchanges.

Data loss and system compromise risks arise when critical vehicle systems fail or are compromised due to the loss or corruption of critical data. Such failures can result in severe consequences, including system shutdowns, accidents, loss of life, and significant financial damage, underscoring the need for robust data backup and recovery procedures. For insurers, system failures caused by data loss may lead to costly claims related to accidents, ultimately increasing claims costs and resulting in higher premiums for policyholders.

Unauthorized access and data exfiltration are pressing concerns as these risks involve attackers gaining unauthorized access to sensitive vehicle data, compromising both vehicle security and safety. This can undermine trust in the connected car ecosystem, compromise data security, and expose sensitive information. Attackers who gain unauthorized access to vehicle data can commit identity theft, steal vehicles, or carry out other malicious activities. Insurers may need to adjust their policies to account for the increased risk of theft or damage caused by compromised systems.

Malware infection and system compromise risks are also prevalent, as vehicles may become infected with malicious software, allowing attackers to execute malicious code and gain unauthorized access to sensitive systems. This can result in loss of control over vehicle functions, exposure of sensitive data, and compromised system security.

System compromise and downgrade risks arise from malicious actors downgrading or disabling critical vehicle systems, which can potentially compromise vehicle safety and performance. This can result in system failure, loss of life, or significant financial losses, underscoring the importance of regular software updates and patching.

System compromise and functionality disruption risks occur when malicious actors target critical vehicle systems, disrupting functionality and endangering safety. This can lead to system failure, injuries, fatalities, or significant financial losses, emphasizing the need for robust anomaly detection and incident response procedures. When such disruptions occur, insurers may have to cover damages or losses, which could drive up claims costs and result in higher premiums for policyholders.

Communication disruption and system compromise risks arise when attackers interfere with critical vehicle communication networks, compromising system security and functionality. This can lead to system failure, loss of life, or significant financial losses, highlighting the importance of implementing secure communication protocols for data exchange. As with other system compromise, communication disruptions can cause accidents or incidents triggered by malfunctioning systems. Insurers may need to revise their policies to reflect the heightened risk of damage or loss resulting from such attacks.

1. Fewer Claims, Higher Payouts

Cyberattacks may be rare, but their impact can be severe, especially when they affect multiple vehicles of critical vehicle functions.

3. Challenges in Profiling New Risks

Cyber risks are poorly represented in historical data and constantly evolving, making them difficult to predict.

2. Change in Policy

Cyber liability insurance becomes crucial as vehicle connectivity exposes OEMs to cyberattacks and data breaches.

4. Difficulty in Determining Liability

Road accidents may stem from driver error or triggered by a cyberattack, complicating the process of assigning liability.

Figure 1.3 Effects of vehicle connectivity on auto insurance

2. The Emerging Auto Insurance Ecosystem

Financial challenges and new market dynamics

Auto insurance policies are designed to provide financial protection against the unexpected costs of road accidents. By paying regular premiums, policyholders receive coverage for a wide range of potential damages, from vehicle repairs to medical expenses. Insurers aim to set premiums that not only cover these costs but also ensure profitability. To achieve this, they rely on analyzing the claims history of a large pool of policyholders, allowing them to assess risk accurately using extensive, real-world data.

However, emerging mobility trends, such as shared mobility, autonomous driving, and vehicle connectivity, are poised to disrupt traditional insurance practices. These new trends lack the vast historical datasets that auto insurers rely on, making it difficult, if not impossible, to apply conventional models for risk profiling. Their technological complexity also complicates the determination of liability in the event of an accident, potentially leading to lengthy litigation if responsibilities are not clear. As a result, the financial viability of auto insurers is at risk. Policy premiums may no longer accurately reflect the actual cost of coverage, while costly litigation could affect profitability.

To address these financial challenges, insurance companies are exploring new strategies, such as usage-based insurance (UBI). This model gives insurers direct access to driver data, allowing them to adjust premiums based on actual driving behavior and assess driver liability in the event of an accident. However, with the rise of new mobility trends, relying on driver data alone is no longer sufficient. Responsibility may not always lie with the driver, as accidents could result from software failures or cyberattacks. As such, insurers must develop a comprehensive understanding of vehicle technologies to profile the new risks accurately and secure access to vehicle data to analyze the most complex liability scenarios.

Since car OEMs and mobility service providers have a thorough understanding of their own technologies and direct access to vehicle data – an advantage that insurers typically lack – they are uniquely positioned to offer their own insurance products. However, they often lack experience in key insurance functions such as determining pricing premiums, handling claims, and navigating regulations across different countries, capabilities that traditional insurance companies have mastered over the years. As a result, the emerging mobility trends can also change the dynamics of the auto insurance market, with insurers, car OEMs, and mobility providers combining their expertise to thrive in this evolving ecosystem.

2.1 New Threats to the Business Model of Auto Insurers

How the emerging mobility endangers the financial viability of insurance companies

The business model of insurance companies, while inherently complex, can be distilled into a simple formula [20]. This formula defines policy premiums, the total amount charged to policyholders for coverage, as the sum of three key factors:

(i) expected losses, which are the payments made when policyholders file claims after an accident; (ii) operational expenses, which include the costs of selling and servicing policies, and the expenses related to handling and settling insurance claims; and (iii) underwriting profit, the margin insurers aim to earn after covering all these costs.

Premiums = (i) Expected Losses + (ii) Operational Expenses + (iii) Underwriting Profit

To set appropriate premiums, auto insurers must accurately estimate the losses from accidents, the costs of handling claims, and their target profits. While it is impossible to predict exactly when an individual will be involved in an accident or how severe it will be, insurers rely on historical data to estimate expected losses. This approach is grounded in the law of large numbers, a statistical principle stating that as the number of policyholders increases, the sample data becomes more representative of the entire population of motorists. This means that the more data is available, the better the predictions about losses become [33].

However, tail-risk events – such as severe multi-vehicle collisions, natural disasters, or cyberattacks – can occasionally occur and have a substantial financial impact on auto insurers. These events involve payouts that far exceed losses and are so rare that there is insufficient data available to profile them accurately. Despite this, auto insurers can remain profitable, as the premiums collected from a large pool of policyholders create a substantial reserve of funds that is sufficient to cover both regular claims and occasional tail-risk events. In other words, the smaller, more predictable claims from the majority of drivers help offset the costs of these rare but high-severity incidents.

Example

Consider an insurance company that covers 100,000 drivers in a specific region. Based on historical data, it expects 500 claims per year, with an average payout of $4,000 per accident. This results in an expected annual loss of $2 million, or $20 per driver when spread across all policyholders. The company also incurs operational expenses of $30 per driver, totalling $3 million. When combined, the total cost per motorist is $50, or $5 million overall.

To remain profitable, the insurance company targets a 20% profit margin, aiming to generate $1 million annually. When distributed among all policyholders, this adds $10 to each premium, bringing the total per driver to $60.

Now, imagine a severe highway flood damages 10 vehicles, with each incurring $20,000 in repairs. The auto insurer would face an additional $200,000 in losses. This unexpected expense would reduce the company's annual profit from $1 million to $800,000, cutting the profit margin by 20%. Despite this tail-risk event, the insurer would still be profitable, demonstrating how a large, diversified policyholder pool helps absorb unexpected, high-cost events.

However, this well-established mechanism that enables insurers to safeguard their financial viability is going to be disrupted by emerging mobility trends. These trends threaten insurers' ability to generate profits in two ways. First, with shared, autonomous, and connected vehicles, the premiums collected by auto insurers may not be sufficient to cover the total claim payouts. These trends, in fact, are expected to significantly increase claim volatility, amplifying the impact of tail-risk events on the finances of auto insurers [18].

To begin with, as discussed in Chapter 1, these trends are expected to reduce the number of accidents. Shared mobility models, for example, could reduce the number of vehicles on the road, resulting in fewer collisions. A similar effect is expected with autonomous vehicles, which aim to minimize driving errors and further decrease the likelihood of accidents. However, these trends will also increase the severity of incidents. Shared mobility may increase the occupancy rate of vehicles, exposing more passengers to the risk of injury in a single accident. Autonomous vehicles are expected to increase repair costs due to their advanced components. Finally, the high level of connectivity in next-generation vehicles introduces new vulnerabilities to cyberattacks, which can result in costly outcomes such as data breaches and ransom demands.

Therefore, while emerging mobility trends are expected to reduce the number of accidents caused by driving errors, currently a source of frequent but low-cost claims, they also increase the likelihood of tail-risk events – rare but high-impact incidents requiring substantial payouts. This shift puts the insurer's profitability at serious risk, as the total premiums collected may not be sufficient to cover the rising costs of these unforeseen events. As a result, auto insurers may face financial losses instead of profits.

Second, with the emergence of new vehicle technologies and shared mobility models, auto insurers may face a significant increase in their operational expenses. These emerging mobility trends make it increasingly difficult for insurers to determine who or what is responsible for an accident, introducing ambiguities that can lead to prolonged and costly litigation [34].

For example, as demonstrated in the previous chapter, determining liability in accidents involving autonomous cars is particularly complex, as responsibility may shift from drivers to the vehicle's OEM or software providers. This could result in disputes over whether the technology failed or the driver failed to intervene. Similar challenges exist in shared mobility models. In car-sharing situations, for example, it may not be clear whether the renter, the vehicle owner, or the car-sharing provider is at fault. Highly connected vehicles also introduce new liability questions, such as whether an accident was caused by driver error or a cyberattack targeting the vehicle's systems.

As a result, emerging mobility trends are expected to drive up costs related to legal fees, administrative resources, and expert witnesses – expenses that will become routine when handling claims. This presents another major financial risk for auto insurers, who now face the dual challenge of increased operational costs and declining revenue, further undermining their financial viability.

To safeguard their profitability, auto insurers will need to revise their strategies. The most straightforward is to increase premiums to offset higher claims payouts and operational costs. However, this approach proves impractical, as it would undermine the competitiveness of auto insurers in the new mobility market. Higher premiums would ultimately drive up the prices of next-generation vehicles and the costs of shared mobility services, pushing potential policyholders to seek more affordable alternatives.

As explained in the previous chapter, the emerging mobility trends are reshaping the insurance landscape, prompting the adoption of policies designed to protect car OEMs and mobility service providers from technological risks, namely commercial auto, product liability, and cyber liability insurance. These policies will not be underwritten directly by vehicle owners or shared mobility users; however, their costs will ultimately be passed on to them, either as part of the final purchase price of vehicles or the cost of shared mobility services. As a result, any increase in premiums will inevitably translate into higher costs for the end user.

This situation will make it even more challenging for autonomous vehicle OEMs, whose technology is still too costly to compete with traditional cars [35] and mobility service providers, whose services remain less cost-effective than private car ownership [36], to succeed in the new mobility market. This means that auto insurers may struggle to attract and retain customers, as car manufacturers and mobility service providers will likely seek lower-cost insurance alternatives to reduce the overall expenses tied to their vehicles and services.

In conclusion, there are no shortcuts. Auto insurers must develop accurate estimates of the losses associated with new types of accidents to ensure that premiums strike the right balance between profitability and market competitiveness. They must also avoid the costly litigation that could arise from ambiguities in determining accident liability, which will allow them to settle claims more efficiently and tightly control their operational expenses. Implementing these measures, however, is not as straightforward as it seems.

For example, estimating potential losses from tail-risk events presents a significant challenge for auto insurers. These events are rare and therefore poorly represented in historical data. As cyberthreats continue to evolve, it will remain difficult to gather enough consistent data to apply the law of large numbers reliably. This makes it essential for auto insurers to develop a comprehensive understanding of the new vehicle technologies and their associated risks. This knowledge will allow them to assess the likelihood and potential impact of incidents beyond traditional statistical models, which are becoming less reliable in the context of new mobility trends.

In addition, avoiding legal disputes over liability is difficult, as insurers' understanding of accident dynamics is still largely limited to driver behavior, often monitored through tools such as on-board diagnostic (OBD) dongles [37]. To properly assess the causes of incidents, auto insurers must also gain access to vehicle data. This information will allow them to determine what happens inside the car, especially as liability will extend beyond the driver to include the vehicle itself and external actors, such as cyber criminals who might attempt to compromise it.

New Insurance Challenges	Corresponding Financial Risks	Solutions to Remain Profitable
New technological risks are difficult to profile These high-payout risks are rare, rapidly evolving, and poorly represented in historical data.	**High risk of incorrectly priced policies** Underpriced premiums may fail to cover total claim payouts, resulting in financial losses instead of profits.	**Knowledge of new vehicle technologies** Understanding how these technologies work enables insurers to assess risks that go beyond driver behavior accurately.
New liability scenarios are difficult to analyze Emerging technologies and mobility models blur responsibility, making it harder to determine who or what is at fault in an accident.	**Potential for lengthy and costly litigation** Legal uncertainty can drive up operational expenses through legal fees, administrative overhead, and expert consultations, further reducing profitability.	**Access to vehicle data** Direct access to vehicle data helps insurers analyze in-car events and detect signs of system failure or cyber incidents.

Figure 2.1 New challenges, financial risks, and potential solutions.

This table summarises the challenges auto insurers will face in the new mobility market, along with the financial risks they pose. It also provides an overview of the solutions insurers must adopt to maintain profitability.

2.2 New Dynamics in the Auto Insurance Market

The emergence of partnerships between auto insurers and vehicle manufacturers

Traditional insurers have held a dominant position in the market for decades, relying on well-established practices to assess the risk of accidents using historical data and assign liability based on individual driving behavior. Today, however, the auto insurance market is on the brink of radical change, as new players are beginning to enter the field. With technological expertise and access to vehicle data becoming crucial for risk profiling and claims settlement, car OEMs find themselves in a surprisingly strong position. Uniquely equipped to understand the technologies they produce, they are increasingly capable of offering their insurance products, potentially challenging the market leadership of traditional auto insurers.

By leveraging their deeper understanding of in-vehicle technologies, car OEMs can develop policies that are better aligned with the risks specific to their products. The same advantage applies to mobility service providers that operate their fleets, as in the case of Lynk&Co. These companies benefit from direct access to real-time vehicle data through built-in connectivity, which enables a more accurate analysis of accident liability. In contrast, traditional insurers typically obtain this data from third-party data sources or devices such as OBD dongles, which provide only partial insights into vehicle behavior. Additionally, by selling insurance policies directly to customers and eliminating intermediaries, car OEMs can reduce operational costs.; Tesla, for example, entered the insurance market in 2019, offering rates 20% to 30% lower than those of traditional insurers [38].

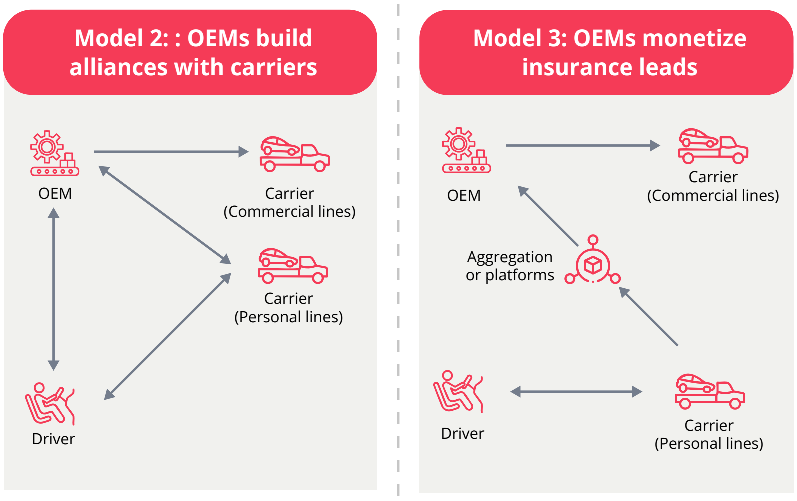
However, what vehicle manufacturers lack is the extensive experience in managing policies and handling claims – an expertise which traditional insurers have perfected over the decades. They also face significant challenges related to regulatory compliance. To operate as insurance providers, manufacturers must obtain the appropriate licences in each jurisdiction [39]: failure to comply can result in legal problems, fines, and reputational damage. Developing this competence is not easy in the short term, as insurance regulations vary widely from country to country. For example, a US-based vehicle manufacturer may be well-versed in North American insurance regulatory frameworks but may lack the same level of knowledge of the regulatory environments in France, China, Brazil, or the other countries where its cars are sold.

As a result, neither insurers nor vehicle manufacturers possess all the capabilities required to thrive in the evolving insurance ecosystem. This gap makes a strong case for collaboration between the two players [40]. By combining the technological expertise and data access of vehicle manufacturers with the regulatory knowledge and operational experience of traditional auto insurers, both parties can create a powerful synergy that significantly enhances their chances of success in the new market. This collaborative approach is already adopted, with partnerships such as that between Toyota and Swiss Re [41], a leading global reinsurance company. Other vehicle manufacturers are beginning to follow this path. Even Tesla, which initially pursued a direct-to-consumer insurance model, partnered with Zurich Insurance in 2024 to offer coverage for its vehicles sold in Australia [42].

As illustrated in Figure 2.2, these new collaborations can take two different forms:

(i) partnerships where vehicle manufacturers manage their own in-house programs with support from traditional auto insurers, or (ii) arrangements in which manufacturers delegate all insurance responsibilities to an external carrier, while sharing information about their technologies and vehicle data through an aggregator.

Regardless of the partnership structure, **neither party fully understands the risks associated with the new vehicle technologies and their vulnerabilities,** highlighting a significant skills gap in the evolving auto insurance ecosystem. These partnerships require a third player: automotive cybersecurity companies.



Model 2: : OEMs build alliances with carriers

OEMs act as intermediaries in personal auto insurance, reducing the total cost of ownership and gaining control over all or part of the insurance customer journey.

Model 3: OEMs monetize insurance leads

OEMs do not sell personal insurance directly but build platforms that enable carriers to offer coverage, sharing vehicle data without owning the insurance journey.

Figure 2.2 Partnership models between insurers and vehicle manufacturers [40]

Along with their respective advantages. However, the figure does not show that both stakeholders still lack a clear understanding of the risks and vulnerabilities associated with new vehicle technologies – knowledge that is crucial for accurately assessing losses and determining

3. The Critical Role of Automotive Cybersecurity

How VicOne can help insurers thrive in the new mobility market

The growing need for technological expertise and access to vehicle data is reshaping the dynamics of the auto insurance market. Insurers are joining forces with car OEMs to enhance the accuracy of their premiums and refine their methods for determining accident liability. However, even with these partnerships, two critical questions remain:

> (i) How can insurers accurately estimate potential losses that can result from accidents if despite having access to information about vehicle technology, they lack a clear understanding of its associated risks?
>
> (ii) How can they accurately determine accident liability if, despite having access to vehicle data, they are unable to interpret this information fully?

As established in the previous chapter, the answer to both questions lies in one essential capability: automotive cybersecurity. To be truly effective, the emerging partnerships between traditional insurers and vehicle manufacturers, must include a third element: automotive cybersecurity companies. Involving automotive cybersecurity experts benefits both parties. For vehicle manufacturers, round-the-clock threat monitoring, prevention, detection, and response reduce risk exposure and ensure compliance with industry standards, leading to lower insurance costs. For auto insurers, leveraging the expertise of automotive cybersecurity professionals enables them to set more accurate premiums based on actual risks and gain valuable insights into liability in the event of an incident, ultimately strengthening their financial viability.

In this scenario, VicOne an automotive cybersecurity leader, stands out as an ideal partner, offering a comprehensive suite of solutions to help vehicle manufacturers reduce their exposure to cyber risks. VicOne's next-generation vehicle security operation center (VSOC), branded as xNexus [45], delivers contextualized automotive threat intelligence that enables manufacturers to detect and respond to security risks in a timely manner while minimizing false alerts. The xCarbon [46], its intrusion detection or prevention system (IDS/IPS), detects or blocks malicious activities, preventing unauthorized access to critical vehicle systems. Additionally, VicOne's Smart Cockpit Protection [47] helps prevent personally identifiable information (PII) and sensitive data stored in in-vehicle infotainment (IVI) systems and companion mobile apps from leaking due to security risks and cyberthreats.

Car OEMs and auto insurance companies can also greatly benefit from VicOne's Zero-Day Vulnerability Database [48], a repository of automotive zero-day vulnerabilities that have been discovered but not yet publicly disclosed – along with VicOne xAurient Action-Ready Automotive

Threat Intelligence. These resources enable OEMs to proactively assess their exposure to emerging threats, such as vehicle theft in underground markets, and share this information with insurers. In turn, insurers can use the insights to more accurately evaluate whether an accident was caused by a cyberattack, including zero-day exploits.

3.1 Leveraging Automotive Cybersecurity to Profile New Vehicle Risks

How VicOne can help auto insurers better determine policy premiums

Establishing partnerships with vehicle manufacturers and gaining access to their knowledge may not be sufficient for auto insurers to profile risks emerging from the new mobility ecosystem accurately. In fact, there is a substantial lack of automotive cybersecurity practiced within the automotive manufacturing industry. According to a global survey by the Ponemon Institute [44], only one in 10 car OEMs has a dedicated automotive cybersecurity team. Additionally, only 44% of OEMs enforce automotive cybersecurity requirements on their suppliers [44], raising serious concerns about how well vehicle manufacturers understand the risks posed by their technologies. As a result, even when OEMs share information with auto insurers, that data may lack the automotive cybersecurity context to assess actual risk exposure, limiting insurers' ability to set accurate, risk-based premiums.

To bridge this gap, insurers must collaborate with automotive cybersecurity companies such as VicOne, which can help them identify potential risks and vulnerabilities.

- When car OEMs use automotive cybersecurity products such as VicOne's xNexus, xCarbon, or Smart Cockpit Protection, they can provide insurers a detailed view of the risks their vehicles are protected against, spanning from electronic control units (ECUs), mobile apps, to back-end systems.
- By using automotive penetration testing services such as VicOne's xScope [49], vehicle manufacturers can provide insurers with insights into the vulnerabilities of their ECUs and IVI systems. They can also share information about the integrity of over-the-air (OTA) updates and potential attack paths in their vehicle communication protocols.
- Insurers could also leverage VicOne's zero-day vulnerability knowledge base, which helps assess whether specific vehicle components are unaffected by undisclosed vulnerabilities.

Armed with these insights, auto insurers will be better equipped to assess technology-related risks and set premiums that more accurately reflect the vehicle's actual exposure to cybersecurity threats. This approach helps ensure that premiums are sufficient to cover potential claim payouts – an essential condition for maintaining viability in the evolving mobility landscape.

3.2 Using Automotive Cybersecurity to Determine Accident Liability

How VicOne can help auto insurers avoid litigation over accident responsibility

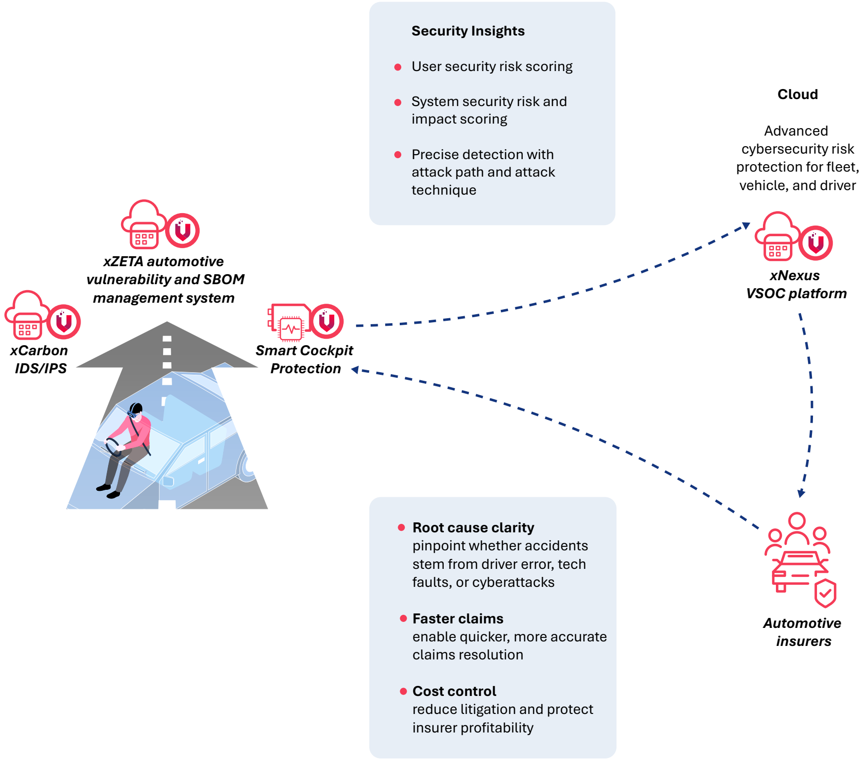
Today, to settle claims after an accident, auto insurers traditionally assess factors such as accident dynamics and driver behavior. These are often evaluated using vehicle-generated data, including diagnostic information and readings from sensors like accelerometers and gyroscopes – data that vehicle manufacturers can readily share with insurers. However, with the emerging mobility trends, auto insurers must also consider technology-related factors. Responsibility for an accident may extend beyond the driver to include the vehicle itself and even external entities like cyber-criminals. This shift requires access to detailed information on the behaviour of vehicle components, on-board software, and the security systems in place.

Access to this information – and the ability to interpret it – is therefore crucial for insurers. Misattributing liability can lead to costly litigation, particularly as legal disputes involving advanced vehicle technologies are likely to extend over long periods, driving up operational expenses. A panel of lawyers at a 2018 conference [21] concluded that only a limited number of experts are capable of interpreting vehicle code and data, and many judges even report feeling overwhelmed by the complexity of such technical testimonies. As these challenges grow, it is becoming increasingly difficult to determine who - or what - bears responsibility for an accident, making it harder for insurers to resolve claims quickly.

It is thus essential for auto insurers to partner with automotive cybersecurity companies like VicOne, which can assist in determining liability following an accident. VicOne can help insurers trace the cause of an incident by leveraging the products used by the vehicle manufacturers. For example:

- **xNexus**, VicOne's VSOC platform, enables insurers to trace the origin of a cyber-attack, identify which components were affected, and determine the intended target of the attack.
- **xCarbon**, VicOne's IDPS, helps detect cyberattacks by monitoring the Ethernet network for suspicious activity and recognising malicious CAN bus messages, such as those with abnormal IDs, payloads, or transmission frequencies.
- **xZETA** [50], VicOne's automotive vulnerability and software bill of materials (SBOM) management system, provides insurers with insights into the vehicle's software stack. This allows them to identify known vulnerabilities in the vehicle's software, such as those in open-source libraries or third-party modules, that may have contributed to the incident.

With the support of automotive cybersecurity, auto insurers will be better equipped to identify the root cause of an accident, whether it is the driver’s behavior, a fault in the vehicle’s technology, a cyberattack, or a combination of these factors. This improved understanding
technology, a cyberattack, or a combination of these factors. This improved understanding
enables faster and more accurate claims resolution, helping insurers avoid prolonged litigation and prevent operational costs from eroding their profits.



Security Insights

- User security risk scoring
- System security risk and impact scoring
- Precise detection with attack path and attack technique

Cloud

Advanced cybersecurity risk protection for fleet, vehicle, and driver

xZETA automotive vulnerability and SBOM management system
xCarbon IDS/IPS
Smart Cockpit Protection
xNexus VSOC platform
Automotive insurers

- **Root cause clarity** pinpoint whether accidents stem from driver error, tech faults, or cyberattacks
- **Faster claims** enable quicker, more accurate claims resolution
- **Cost control** reduce litigation and protect insurer profitability

Fig. 3.1 How VicOne adds value to Auto Insurers-OEMs partnerships.

This figure shows how auto insurers can benefit from automotive cybersecurity, even without directly using VicOne products, through their collaboration with vehicle manufacturers.

Recommendations

The auto insurance market is undergoing a major transformation, driven by trends such as shared mobility, autonomous vehicles, and vehicle connectivity. These trends will drive auto insurers to forge strategic partnerships with car OEMs, as setting accurate premiums and determining liability now depend on a deeper understanding of vehicle technologies and access to relevant data. However, these partnerships face a major limitation: neither insurers nor vehicle manufacturers have a clear and comprehensive grasp of the risks and vulnerabilities associated with the new technologies. Without this understanding, insurers risk underpricing policies and facing costly, protracted legal disputes – both of which threaten their financial viability.

To adapt to the emerging mobility ecosystem, we recommend that both OEMs and auto insurance providers integrate automotive cybersecurity into their operations. Automotive cybersecurity capabilities will play a crucial role in these new partnerships, providing benefits for both parties:

- **Vehicle manufacturers**, as well as mobility service providers, should adopt robust automotive cybersecurity solutions to protect passengers, drivers, and other road users. By reducing their exposure to cyber and technology-related risks, they can also lower their insurance costs.
- **Auto insurance companies** should prioritize partnerships with vehicle manufacturers that implement robust automotive cybersecurity measures. These solutions will enable insurers to accurately profile emerging threats and set premiums that reflect the actual risk level. Additionally, automotive cybersecurity will support liability assessments, reducing the likelihood of legal disputes and helping to control operational costs.

In conclusion, we invite readers to visit **VicOne's official website** [43] and explore their comprehensive suite of automotive cybersecurity solutions. By integrating these tools into their operations, both vehicle manufacturers and auto insurers will be better equipped to stay ahead of emerging threats, improve risk management, and thrive in the new mobility ecosystem.

References

[1] https://www.swissre.com/institute/research/sigma-research/Insurance-Monitoring/us-property-casualty-outlook-january-2024.html

[2] https://onlinepubs.trb.org/onlinepubs/trnews/trnews259billioncars.pdf

[3] https://www.thedrive.com/guides-and-gear/how-many-cars-are-there-in-the-world

[4] https://www.oliverwyman.de/content/dam/oliver-wyman/v2/publications/2023/nov/2023-oliver-wyman-shared-mobility-report

[5] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-squaring-risk-in-the-sharing-age.pdf

[6] https://onlinelibrary.wiley.com/doi/full/10.1111/rmir.12140

[7] https://www.tandfonline.com/doi/full/10.1080/01944363.2015.1057196

[8] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-future-of-mobility-mobility-evolves

[9] https://www.mdpi.com/2071-1050/13/13/7384

[10] https://www.marshcommercial.co.uk/for-business/commercial-vehicle-insurance.html

[11] https://link.springer.com/article/10.1007/s11116-018-9923-2

[12] https://www.sciencedirect.com/science/article/abs/pii/S0968090X18307551

[13] https://insurance-edge.net/2023/11/01/why-insurance-is-a-challenge-for-the-shared-mobility-sector/

[14] https://vicone.com/blog/from-key-fob-to-uwb-explaining-and-securing-ultra-wideband-in-vehicles

[15] https://www.sae.org/blog/sae-j3016-update

[16] https://press.spglobal.com/2023-09-25-Autonomous-Vehicle-Reality-Check-Widespread-Adoption-Remains-at-Least-a-Decade-Away,-according-to-S-P-Global-Mobility

[17] https://www.theverge.com/23948708/cruise-robotaxi-suspension-trust-remote-assist

[18] https://onlinelibrary.wiley.com/doi/full/10.1111/rmir.12168

[19] https://crashstats.nhtsa.dot.gov/Api/Public/Publication/812115

[20] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-insurance-in-the-new-mobility-ecosystem.pdf

References

[21] https://gould.usc.edu/why/students/orgs/ilj/assets/docs/32-1-Rustad.pdf

[22] https://www.theguardian.com/us-news/2023/jun/07/waymo-car-kills-dog-self-driving-robotaxi-san-francisco

[23] https://www.aig.sg/content/dam/aig/apac/singapore/documents/other/aig-the-future-of-mobility-and-shifting-risk.pdf

[24] https://www.tandfonline.com/doi/full/10.1080/01441647.2018.1494640#d1e291

[25] https://focalpointpositioning.com/insights/gps-spoofing-a-cyber-security-threat-to-in-car-navigation-avs

[26] https://dl.acm.org/doi/10.1145/3558482.3590192

[27] https://www.mdpi.com/2624-800X/3/3/25

[28] https://vicone.com/research/the-road-ahead-is-paved-with-risky-data

[29] https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/

[30] https://www.forbes.com/sites/stevetengler/2023/10/25/new-auto-cyber-study-reveals-threat-intelligence--or-lack-thereof/

[31] https://www.ibm.com/reports/data-breach

[32] https://resources.trendmicro.com/Connected-Cars-Research

[33] https://www.investopedia.com/articles/personal-finance/081616/behind-law-large-numbers-insurance-industry.asp

[34] https://www.cov.com/en/news-and-insights/insights/2023/11/insurance-for-autonomous-vehicles-who-will-drive-those-risks

[35] https://www.forbes.com/sites/johanmoreno/2021/01/22/waymo-ceo-says-tesla-is-not-a-competitor-gives-estimated-cost-of-autonomous-vehicles

[36] https://www.simon-kucher.com/en/insights/car-subscriptions-trend-thats-here-stay

[37] https://ims.tech/knowledge-hub/insurance-telematics-service-providers-obd2-device/

[38] https://www.tesla.com/sv_se/blog/introducing-tesla-insurance

[39] https://www.gov.uk/find-licences/authorisation-to-advise-on-or-arrange-general-insurance

References

[40] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/navigating-unknowns-auto-insurance-questions-in-a-new-mobility-era

[41] https://www.swissre.com/media/press-release/nr-20200921-toyota-insurance-services-to-join-swiss-re-adas-risk-platform.html

[42] https://www.zurich.com.au/latest-news/media-releases/2024/insuremytesla-agreement-announced-between-zurich-and-tesla.html

[43] https://vicone.com/

[44] https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_ the_modern_ vehicle.pdf

[45] https://vicone.com/products/xnexus

[46] https://vicone.com/products/xcarbon

[47] https://vicone.com/solutions/smart-cockpit-protection

[48] https://vicone.com/automotive-zero-day-vulnerabilities

[49] https://vicone.com/products/xscope

[50] https://vicone.com/products/xzeta

VicOne

Driving Automotive Cybersecurity Forward

IN COLLABORATION WITH

TREND MICRO™ Trend Research