VicOne | HSB
A Munich Re company

Beyond the Vehicle: How Automotive Cyber Risk Extends Across Business Operations and Supply Chains

Learn more about VicOne by visiting **VicOne.com** or scanning this QR code:

Executive Summary

Connected commercial vehicles are becoming integral to how businesses coordinate employees, deliver goods and services, and manage daily operations. Through telematics, fleet management platforms, mobile applications, over-the-air updates, and cloud services, vehicles now exchange information with systems and organizations far beyond their physical boundaries. This connectivity creates operational advantages, but it also allows automotive cyber risk to reach beyond the affected vehicle.

In 2025, VicOne recorded 610 automotive cybersecurity incidents, including 161 cross-region and multi-business incidents. VicOne's findings show that automotive cyber incidents span in-vehicle systems, cloud services, enterprise IT, and other connected environments.[1] As these domains converge, a vulnerability or compromise affecting one part of the ecosystem may have consequences across several systems, business units, or locations.

For businesses that depend on commercial vehicles, the consequences may range from the loss of a single vehicle to broader disruptions to fleet and business operations. Yet the nature and scale of these losses may not be fully captured if connected vehicles are viewed solely as transportation assets, or if automotive and enterprise cyber risks are assessed separately.

Developed by HSB in partnership with VicOne, this paper examines how automotive cyber risk can extend across commercial vehicles, business operations, and supply chains. By connecting the technical origins of automotive cyber incidents to their operational and financial consequences, the paper aims to provide businesses and insurers with a clearer basis for understanding an exposure that extends beyond the vehicle.

Chapter 1. The Connected Vehicle Threat Landscape at a Glance

Connectivity is one of several trends, alongside autonomous driving, electrification, and shared mobility, reshaping how transportation is delivered and used.[2] In commercial transportation, this shift is already visible as vehicles exchange data with fleet management platforms, mobile applications, cloud services, and other systems used to coordinate daily operations. This integration turns the vehicle from a mode of transportation to a connected operational endpoint.

The result is an automotive attack surface that extends beyond systems installed by the vehicle manufacturer. It may include aftermarket devices, driver smartphones, wireless interfaces, fleet software, and third-party services. A weakness in any of these elements may affect the vehicle or the information the business relies on.
This chapter provides an overview of the technologies on which connected commercial vehicles depend, the paths through which they may be compromised, and the objectives threat actors may pursue.

1.1 Commercial vehicles as connected operational assets

From vehicle data to business decisions

Businesses use connected vehicle data to manage routes, drivers, maintenance, deliveries, and customer services. A service vehicle may receive appointments and navigation instructions through a driver application, while a truck may transmit its location, condition, shipment information, and driver status to a fleet platform.

This information supports decisions about where a vehicle should go, whether a driver can continue a trip, and whether the vehicle should remain in service. A cyber incident does not have to affect steering, braking, or any other vehicle functions to disrupt operations. Losing access to operational data or being unable to trust its accuracy may be enough.

ELDs illustrate the wider interdependencies

Electronic logging devices (ELDs) show how a vehicle function can depend on systems beyond the installed device. Under the U.S. Federal Motor Carrier Safety Administration (FMCSA) rules, an ELD synchronizes with a commercial vehicle's engine to record driving time and duty status. The record may also depend on a mobile application, cloud service, device communications, user accounts, and vendor technology.[3]

VicOne's CyberThreat Research Lab reviewed 17 Android ELD applications and identified recurring concerns across these layers.[4] The findings showed that the integrity of an electronic log depends not only on the ELD but also on the applications, backend services, communications, vendor technologies, and access controls that support it.

1.2 Multiple paths into the connected vehicle environment

An automotive cyber incident may begin through a vehicle interface, a connected device, a centralized platform, or a trusted software provider.

Vehicle interfaces

Cellular, Wi-Fi, Bluetooth, USB, and on-board diagnostic interfaces connect vehicles to external systems and devices. The U.S. National Highway Traffic Safety Administration (NHTSA) identifies these wired and wireless connections as potential entry points. Its guidance notes that an aftermarket telematics device collecting fleet data could, depending on the vehicle architecture, provide a path to other vehicle systems.[5]

The risk depends on how the vehicle processes external data, what access the interface provides, and whether the exposed system is adequately separated from other domains.

From guest Wi-Fi to fleet systems

At DEF CON 33, researchers demonstrated how a transit bus's guest Wi-Fi could become the starting point for broader system access. By combining a known router vulnerability with weak credentials, plaintext services, and exposed directories, they reached live camera feeds, GPS data, vehicle-status information, backend fleet and route pages, and a vendor's remote server.[6]

The exploit showed how data introduced through a familiar physical interface can exploit weaknesses in complex infotainment software. Although segmentation may limit access to safety-critical functions, a compromise of the infotainment layer can still expose sensitive information, disrupt connected services, and lead to operational or reputational consequences.

Connected devices and applications

Commercial vehicles may connect to telematics equipment, tracking devices, driver smartphones, and other aftermarket technologies. These tools may contain credentials, route data, or access to external services. A weakness in an application, user account, communication channel, or supporting backend service may expose information or provide access to another part of the connected environment.

The risk introduced by aftermarket devices is not hypothetical. In 2026, researchers found that dealer-installed KARR/SWDS anti-theft devices in at least 2.2 million vehicles relied on the same security key. An attacker within Bluetooth range could unlock doors or prevent a vehicle from starting, demonstrating how a single third-party device can create shared exposure across multiple vehicle brands.[7]

Fleet and cloud platforms

Fleet management and dispatch platforms centralize information and access across multiple vehicles. Compromise of an account or backend system could interfere with tracking, scheduling, dispatch, or communications without requiring an attacker to target each vehicle separately.

In 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) disclosed CVE-2025-4364 [8], a vulnerability in the Assured Telematics fleet management system that could expose sensitive system information beyond its intended scope.[9] The advisory illustrates how risk may reside in the centralized platform as well as the vehicle.

Software updates and third-party dependencies

Connected vehicles rely on software and services from manufacturers and other technology providers. A compromise of an over-the-air (OTA) update process or another trusted channel could allow unauthorized software to reach multiple vehicles. VicOne identifies fleet-scale OTA compromise as an emerging risk because centralized infrastructure can magnify a breach's impact.[10]

These paths may intersect. The potential impact depends on the access gained through the initial compromise and the other vehicle, fleet, and business systems connected to it.

1.3 Threat scenarios and attacker objectives

The same vulnerability can support different objectives depending on the system compromised and the access obtained. These scenarios fall into three general categories: operational disruption and extortion, data compromise, and unauthorized vehicle access.[11]

Threat objective	Potential attacker action	Immediate effect
Operational disruption and cyber extortion	Deploy malware, disable or downgrade a vehicle function, interfere with communications or a connected service, disrupt a fleet platform, or demand payment to restore access	Vehicle or system unavailability, loss of fleet visibility, and interruption of dispatch or other connected functions
Data theft and exfiltration	Access or steal driver identities, customer information, locations, route histories, vehicle credentials, or maintenance records	Exposure of sensitive information and possible misuse of vehicle or business data

Data manipulation	Alter, delete, corrupt, or inject false vehicle, location, delivery, or maintenance data	Loss of confidence in the information used to make operational decisions
Unauthorized access and vehicle theft	Compromise digital keys, connected access systems, vehicle credentials, infotainment systems, telematics, or aftermarket devices	Unauthorized entry, loss of vehicle access or control, vehicle theft, or a pathway to other connected systems

Table 1. Common connected vehicle threat objectives, potential attacker actions, and immediate effects.

The significance of an incident depends not only on the attacker's initial access or objective, but also on the vehicle functions, shared platforms, data, and business activities connected to the affected system. Chapter 2 examines how these threats can lead to immediate business interruption and broader organizational and supply chain consequences.

Chapter 2. From Vehicle Compromise to Business Disruption

The operational impact of an automotive cyber incident depends not only on how many vehicles are affected, but also on the activities, systems, and external commitments that rely on them. One unavailable vehicle may disrupt a specialized service, while a compromised fleet may interrupt operations across many otherwise functional vehicles.

This chapter traces how these effects can extend from immediate vehicle downtime to fleet-wide disruption, sensitive data compromise, and broader organizational and supply chain consequences.

2.1 One vehicle can interrupt an operation

Loss of availability

A cyberattack affecting just one commercial vehicle can create an immediate business problem. The vehicle may fail to start, lose access to a connected function, provide unreliable data, or need to be taken out of service while the incident is investigated.

A disabled service van may prevent a technician from reaching customers, while an unavailable delivery vehicle may cause the business to miss a delivery window. A vehicle carrying specialized equipment may also be more difficult to replace than its market value suggests.

Costs surrounding the downtime

The financial impact may include towing, diagnostics, system restoration, temporary transportation, employee downtime, and lost income. A replacement vehicle may also require specialized equipment before it can perform the same function.

The impact generally increases when:

- The vehicle performs a specialized or time-sensitive function.
- No replacement vehicle is immediately available.
- Downtime exceeds what can be managed through rescheduling.
- The affected vehicle is critical to operating capacity.

2.2 Shared systems can increase the scale of disruption

When vehicles share a fleet platform, software, credentials, or connected service, an attacker may not need to compromise each vehicle individually. Disrupting the shared system may be enough to affect operations across the fleet.

A fleet platform outage may interrupt:

- Vehicle tracking and availability
- Dispatch and driver assignments
- Reservations and scheduling
- Maintenance and inspection records
- Driver communications

The vehicles may remain physically operable, but the business may lack the information needed to use them efficiently. Manual workarounds can preserve some activity, usually with less visibility and capacity.

If attackers deny access and demand payment to restore the system, the downtime itself becomes leverage.

When a fleet platform becomes unavailable

In April 2026, a cybersecurity incident led Chevin Fleet Solutions to take affected FleetWave environments offline. FleetWave is a platform designed to centralize vehicle, driver, maintenance, compliance, and other operational information.

The outage affected Missouri's state fleet management system. Agencies were instructed to use telephone workarounds for vehicle reservations and reservation status checks.[12]
The incident was not reported as a compromise of the vehicles themselves. It nevertheless illustrates how the loss of a shared platform can disrupt fleet-related workflows even when vehicles remain physically available.

2.3 Sensitive data can be lost, exposed, or manipulated

Connected commercial vehicles and their supporting platforms may process driver and customer information, location histories, delivery records, duty status, maintenance data, and application credentials. A cyber incident can affect the confidentiality, integrity, or availability of this information.

Confidentiality

Attackers may steal information to commit fraud, extort, steal vehicles, or gain further access to business systems. Location and route data may also reveal where vehicles, employees, customers, or valuable goods are likely to be at a given time.

Integrity

Manipulated route, delivery, duty status, vehicle condition, or maintenance data can lead to incorrect operational decisions. VicOne's ELD research shows that data integrity depends on several connected layers, including applications, cloud services, device communications, vendor technology, and access controls.

Availability

Even when data is neither stolen nor altered, loss of access may prevent dispatchers, drivers, maintenance teams, and managers from performing their work. In an extortion event, this unavailability may become leverage. Data compromise may also create identity-recovery, notification, legal, regulatory, and reputational costs.

Data compromise can have consequences far beyond the affected information or systems. In 2023, KNP Logistics, a 158-year-old UK transport company, suffered a ransomware attack after attackers gained access through a weak employee password. Locked out of the data needed to operate, the company ultimately closed, costing approximately 700 people their jobs.[13]

2.4 Consequences can extend across the organization and supply chain

Organizational consequences

Vehicle downtime, fleet platform interruption, and data compromise may lead to lost revenue, emergency expenses, customer complaints, contractual issues, privacy obligations, and reputational damage.

A cyberattack does not have to take cars off the road to impact transportation. In July 2026, Nihon Kotsu, a Japanese taxi operator, disclosed that unauthorized access and malware had disrupted its telephone dispatch service, web-based chauffeur bookings and reservations, and some internal systems. Registration for its specialized maternity taxi service was also suspended. While taxis remained available through a separate app or could be hailed, the incident directly disrupted the systems connecting customers with those vehicles. [14]

The effects of incidents of this kind may continue long after access is restored. Businesses may need to clear backlogs, verify records, communicate with customers, and investigate whether other systems were affected.

Supply chain consequences

Supply chain effects arise when another organization depends on the affected vehicle or service. A delayed shipment may leave a warehouse without inventory, a production line

without components, or a customer without equipment needed for its own operations. A service vehicle that fails to reach a site may delay maintenance, construction, or another scheduled activity.

Supply chain consequences are more likely to escalate when:

- Goods or services are time-sensitive
- Backup inventory is limited
- The vehicle or its equipment is difficult to replace
- Delivery windows are tightly coordinated
- Alternate carriers or manual processes are unavailable

A cyberattack does not need to immobilize an entire fleet to produce wider consequences. One specialized vehicle may support a critical activity, while one compromised platform may affect many otherwise operational vehicles. Severity is shaped not only by the number or value of the affected assets, but also by the revenue, data, services, and external commitments that depend on them.

The next chapter examines how businesses and insurers can evaluate this exposure and the complementary roles of automotive cybersecurity, business continuity, and commercial auto cyber insurance.

Chapter 3. Connecting Automotive Cyber Risk to Business Resilience

The scale of a connected vehicle loss depends not only on the technical severity of the incident or the number of vehicles affected, but also on the operations, systems, and external commitments that rely on them.

This chapter examines why the risk is difficult to assess and how technical, operational, and financial perspectives can provide a more complete view.

3.1 Why connected vehicle cyber risk is difficult to assess

Limited historical data

Insurance models traditionally rely on historical claims data to estimate future losses. VicOne's white paper, "Insuring the Future of Mobility," noted that connected vehicle cyber risks challenge this approach because they are relatively new, rapidly evolving, and underrepresented in established loss records.[15]

The absence of frequent claims does not necessarily indicate low exposure. New vulnerabilities may emerge after a vehicle enters service, while zero-days and other weaknesses may not immediately appear in formal vulnerability databases or conventional risk processes.[16] Shared software and centralized platforms can also allow one incident to affect multiple vehicles or businesses.

Operational severity depends on context

The same technical incident can produce different losses across businesses. Its severity depends on the affected vehicle's function, reliance on shared systems, availability of replacements, expected recovery time, sensitivity of the data involved, and customer or supply chain commitments. Vehicle value alone does not provide a complete picture of exposure.

Responsibility is distributed

Responsibility for connected vehicle technology is often distributed across manufacturers, software and service providers, fleet operators, and insurers, while ownership and accountability remain divided.[17] When responsibilities are divided, it can be unclear who monitors vulnerabilities, maintains affected systems, responds to incidents, or supports recovery. This lack of accountability may also complicate investigation and claims handling when available information does not clearly distinguish mechanical failure, software malfunction, operational error, and malicious activity.

3.2 Visibility must extend beyond the vehicle

A more complete assessment connects three views of the exposure: technical, operational, and financial.

Technical visibility

Businesses need to understand which technologies connect their vehicles to external systems. These may include factory-installed software, aftermarket devices, mobile applications, fleet platforms, wireless interfaces, OTA services, and third-party dependencies.

Relevant questions include:

- Which vehicles and systems share software, credentials, or backend services?
- Which interfaces and third-party services could provide external access?
- Which vulnerabilities and attack paths could affect several vehicles or systems?

Vehicle and fleet data do not automatically explain whether an event resulted from ordinary failure or malicious activity. Automotive threat intelligence, vulnerability analysis, penetration testing, and security monitoring can provide the context needed to interpret that information.

Operational visibility

Technical information must be connected to how the business uses its vehicles. This includes understanding:

- Critical or time-sensitive activities supported by vehicles
- Tolerance for vehicle or platform downtime
- Availability of replacement vehicles and manual processes
- Customer, third-party, and supply chain dependencies

Financial visibility

Financial assessment should account for direct recovery costs, lost income, additional expenses, data-related costs, and contractual consequences arising from the interruption. The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 organizes cybersecurity outcomes into six Functions: **Govern, Identify, Protect, Detect, Respond**, **and Recover**. It places these outcomes in the context of an organization's mission, stakeholders, and supply-chain relationships.[18] For connected vehicles, this supports aligning technical controls with continuity and financial recovery planning.

3.3 Vehicle cyber incidents may fall between conventional coverage

Businesses may assume that a vehicle warranty, a commercial auto policy, or a general cyber policy will respond to a connected vehicle cyberattack. In reality, these mechanisms serve different purposes, and their treatment of vehicle-based cyber incidents may vary. A vehicle warranty generally addresses specified defects or failures rather than the broader financial fallout of a cyberattack. A conventional commercial auto policy tends to focus on physical damage, liability, and established vehicle risks without addressing cyber events. And a general cyber policy, while covering enterprise systems and data, may exclude vehicles or losses originating from vehicle systems altogether. The result is uncertainty around exactly who pays for vehicle system and data restoration, lost business income, temporary transportation, loss of use, extra expenses, cyber extortion response, and identity recovery.

"Silent cyber" for connected vehicles

The insurance industry has a name for the resulting uncertainty, and it's one the property and casualty (P&C) sector has grappled with before: "silent cyber." The term refers to the risk that cyber-related losses trigger coverage under traditional policies that were never explicitly written to address cyber risk — neither affirmatively covered nor excluded. It became a major industry concern after events like NotPetya in 2017,[19] when malware caused billions in losses across property and GL lines whose policy language had never contemplated networked causes of loss, leaving insurers exposed to unpriced, unquantified aggregation risk. The industry responded by pushing explicit cyber exclusions or affirmative endorsements across most commercial lines.

Commercial auto now faces a similar exposure as vehicles grow more connected and software-dependent. Traditional auto forms simply weren't drafted with today's cyber risks in mind, and since most still lack clear cyber exclusions, insurers face the same kind of silent, non-affirmative exposure that caught property and GL lines off guard pre-2017. Explicit cyber carve-outs or endorsements look like the industry's next logical step — and ISO is already moving in that direction, having recently introduced an "Auto Hacking" endorsement to provide affirmative coverage for specified cyber incidents. Many carriers adopting the new form have opted to include this coverage, citing an industry-wide push to get ahead of the silent cyber issue. As a result, purpose-built commercial auto cyber coverage has begun to emerge, aimed squarely at these vehicle-related exposures.

Because coverage varies so much from policy to policy, businesses shouldn't assume vehicle-based cyber events are included or excluded — they should review the terms, conditions, limits, and exclusions that apply to them. The Federal Trade Commission offers similar guidance, advising businesses to assess which first- and third-party losses a cyber policy covers and whether that fits their organization's needs.[20]

For insurers, clearer treatment of connected vehicle cyber risk means less silent exposure and more informed underwriting and claims handling. Because this is such a new coverage area, claims should be handled by examiners with dedicated cyber claims experience. These adjusters have experience navigating the unique and complex losses that arise from cyberattacks, which positions them to respond more effectively than adjusters whose expertise is primarily in commercial auto claims.

The role of claims in supporting cyber risk for connected vehicles

Traditional cyber policies center on coverages such as cyber extortion, business income loss, identity recovery, and system restoration — areas that dedicated cyber adjusters work with every day. Many of these core cyber coverages are included in some of the affirmative commercial auto cyber policies in circulation today. Moreover, cyber claims adjusters know which vendors to bring in for extortion negotiation and payment, and they're practiced at reviewing coverage triggers and mapping them to the right coverage, making the claims process more effective.

Business income loss is one of the most critical coverages in this space, and it's directly relevant to commercial auto businesses like trucking fleets, delivery operators, and rideshare companies. A cyber incident doesn't need to cause a crash to shut down operations: telematics outages, ransomware locking fleet management software, or a compromised ELD network can ground vehicles just as effectively as physical damage. Even a few days of downtime translates into real revenue loss — but proving and calculating that loss is far more complex than a standard commercial auto claim.

This is where cyber-specific adjusters have an edge. Calculating business income loss means reconstructing what the business would have earned absent the incident, along with the extra expenses incurred to keep operations running. It's a different exercise than estimating repair costs or liability exposure — and dedicated cyber adjusters assess these types of losses every day.

That is why many cyber insurers supplement their teams with forensic accounting firms on retainer or in-house, specializing in building the loss methodology, validating financial records, and defending the number if disputed. With that expertise informing their review, cyber claims adjusters are able to make the final determination quickly and confidently. For commercial auto businesses increasingly dependent on connected vehicle technology, that combination can be the difference between a claim resolved fairly and one that drags on or under-delivers.

When an automotive cyber incident affects another business

A 2025 cyber incident at Jaguar Land Rover disrupted the automaker's operations for almost six weeks and affected organizations that relied on its systems and supply chain.[21] Vertu Motors, which operated 10 Jaguar Land Rover dealerships, estimated that the disruption could reduce its fiscal year earnings by up to £5.5 million.[22]
Vertu indicated that it would explore a claim under its insurance policy, which included business interruption coverage for third-party system outages. Public reporting did not confirm whether the claim was ultimately submitted, accepted, or paid.
The JLR case illustrates a relevant coverage question: when a cyber incident occurs elsewhere in the automotive ecosystem, losses may arise at businesses whose own systems were not directly attacked. Connected fleets create a similar dependency when vehicles rely on external software, fleet platforms, manufacturers, or service providers.

3.4 Cybersecurity, continuity, and insurance provide complementary perspectives

The Insuring the Future of Mobility white paper also identified a gap between access to vehicle information and the cybersecurity expertise needed to interpret associated threats and vulnerabilities. For connected commercial vehicles, this assessment also requires knowledge of the operations that depend on the affected vehicle.

Fleet-reliant businesses, automotive cybersecurity specialists, and insurers contribute to different parts of the risk picture.

Fleet-reliant businesses

Businesses hold the operational picture that neither cybersecurity providers nor insurers can supply: which vehicles support which commitments, what downtime the organization is able to absorb, and which external relationships depend on continued service. They are also positioned to act on a significant part of the resulting exposure. Chapter 4 covers what that involves.

Automotive cybersecurity specialists

Even though some of the threats faced by connected vehicles are similar to other cyber-related threats, they require unique insights into this new threat landscape. Automotive cybersecurity leaders such as VicOne deliver purpose-built security solutions for in-vehicle networks, embedded ECUs, and software-defined architectures, rather than adapting general IT tools. Drawing on dedicated automotive threat intelligence, VicOne supports a vehicle's entire life cycle, from development through operation and maintenance.

Insurers

HSB Commercial Cyber for Auto is designed to help small and medium-sized businesses recover from disruptions caused by auto-related cyberattacks. HSB Commercial Cyber for Auto also can pay for transportation costs, including towing, labor, and loss of use of vehicles, while cybersecurity services provide online resources to help stop cyberattacks. Should an attack occur, HSB Commercial Cyber for Auto includes the cost to improve or upgrade hardware and software to help prevent future cyber incidents.

Figure 1. ***Connecting the three views of automotive cyber risk.*** *Operational dependencies, cyber exposure, and potential financial and recovery needs converge around the connected vehicle.*

No single perspective is sufficient on its own. Cybersecurity can reduce the likelihood or severity of an incident, but it cannot eliminate every vulnerability, third-party failure, or emerging threat. Insurance can support financial recovery, but it does not prevent disruption or restore operations on its own. Business continuity connects both perspectives to the activities that must continue.

Together, these perspectives provide a clearer view of both the likelihood and potential severity of a connected vehicle cyber incident.

Chapter 4. What Fleet-Reliant Businesses Can Control

Chapter 3 described an exposure where responsibility is distributed across manufacturers, software and service providers, fleet operators, and insurers. That distribution is real, and it can leave businesses with the impression that connected vehicle risk sits largely outside their control.

Much of it does not. The vehicle-specific parts of this exposure belong to manufacturers and specialist providers, but the paths described in Chapter 1 do not stop at the vehicle. They run into fleet platforms, cloud services, user accounts, and vendor relationships, which are ordinary enterprise systems that happen to have vehicles attached to them. Businesses already manage risk in systems like these everywhere else in their operations. What tends to be missing is that connected vehicles have not been brought inside that same management.

This chapter covers what that involves. It maps broadly to the Protect, Detect, Respond, and Recover functions of the NIST CSF 2.0 framework referenced in Chapter 3.

4.1 Bring the fleet inside the security program

Fleet technology often gets procured, administered, and supported outside the processes a business applies to the rest of its IT environment. It may be selected by operations rather than by IT, supported by a vendor rather than an internal help desk, and left out of the inventories, access reviews, and assessments that cover everything else. The result is a set of business-critical systems that nobody has assessed as business-critical. Three measures address most of this.

Account control. Fleet platforms concentrate access across multiple vehicles at once, which is exactly why managing who holds an account, and what that account is able to do, gives businesses more leverage than almost anything else available to them. The failure patterns will look familiar to anyone who has run into them in other business systems: shared logins that make it impossible to tell who did what, service and integration accounts that get exempted from multi-factor authentication, credentials handed to a vendor for one engagement and never turned off, and administrative access granted to people who only needed to pull reports. The KNP incident described in Chapter 2 reportedly started with one weak employee password.

Inclusion in assessment. Security assessments, vulnerability scanning, and access reviews should cover fleet platforms and their supporting accounts on the same schedule as other business systems. Where a platform is vendor-hosted and cannot be tested directly, documented assurance from the provider serves the same purpose.

Third-party diligence. Concentration risk gets created at procurement and then inherited for the life of the contract, and the platform outage described in Chapter 2 shows what that looks like in practice. The questions are the same ones a business should be asking of any critical vendor: whether the platform supports single sign-on and enforces multi-factor authentication, including on the vendor's own support access; what the breach notification commitment is; which subprocessors handle fleet or driver data; and whether the business could keep operating for 72 hours without the platform. That last question is addressed in Section 4.4.

Aftermarket hardware is worth calling out separately, because it gets procured the least formally and reviewed the least often. The KARR/SWDS exposure in Chapter 1 involved devices that dealers installed across millions of vehicles. Most businesses will not be positioned to evaluate a device like that technically, but they can still ask who supports it, what data it collects and where that data ends up, and how the manufacturer handles security updates.

4.2 Extend awareness to a workforce that is not at a desk

Security awareness training generally assumes an employee with a corporate laptop, an email account, and a service desk to call. A large part of a fleet workforce has none of those. Their working environment is a mounted device, a mobile application, and a vehicle that sits in unsecured locations and gets accessed by third parties for maintenance and repair. In this environment, an anomaly that nobody is trained to route is an anomaly nobody sees.

Drivers are the people positioned to notice. A corporate endpoint has monitoring software watching it; a vehicle has the person operating it. Training should reach past reporting suspicious email and into reporting anything unexpected in the equipment: a device behaving abnormally, information displaying incorrectly, an unprompted request to install or approve something, or hardware showing up on the vehicle that nobody scheduled. Drivers do not need to diagnose any of this. They only need to report it.

The escalation path is the real deliverable. Awareness without a route to act on it changes nothing. Observations like these currently reach dispatch or maintenance, where they get handled as equipment complaints and go no further. Deciding what gets escalated, who receives it, and how patterns across several vehicles become visible is the piece most businesses have not built. Yet this costs very little to build.

Dispatchers warrant separate attention. Dispatch staff usually hold administrative access to the fleet platform, which makes them a proportionate target for the same social engineering used against privileged users in any organization: a caller presenting as vendor support and asking someone to approve an authentication prompt, or a request to confirm account credentials.

Some populations sit outside the training program altogether. Owner-operators, leased drivers, and subcontracted carriers may hold platform access without ever being employees, which tends to leave them out of both training and access reviews.

Delivery should follow existing practice. Fleet operators already run effective training infrastructure for safety and compliance. Brief material delivered through channels drivers already use and framed as an uptime and safety matter rather than an IT requirement will hold far better than an annual module.

4.3 Recognize that disruption is preceded by a window

Ransomware and similar events are not instantaneous. Encryption or lockout is the final stage of an intrusion that usually involves a period of access, exploration, escalation of privilege, and interference with backups. The interval between the initial compromise and the loss of operations is where the eventual severity gets determined, and it generally runs longer than businesses assume.

That interval matters more for smaller fleet-reliant businesses, not less. Few of them maintain a security operations function, so the practical question is never whether a system can generate an alert. It is whether anyone actually receives it. Several of the relevant signals already get produced by the platforms these businesses use: changes to administrative access, unusual volumes of data leaving the system, authentication from unfamiliar locations, and modifications to backup settings. Confirming which of these a platform can alert on, and then turning them on, is a configuration exercise rather than an investment.

Businesses should establish who receives an alert like that outside working hours, and what that person is authorized to do: suspend an account, disable an integration, or call the vendor. Where the internal capacity does not exist, this can be sourced from the platform provider, a managed security provider, or an insurer's pre-incident services.

The distinction matters. An intrusion caught inside this window is an incident. The same intrusion caught after encryption is a business interruption, and Chapter 2 describes what that has cost businesses that got there.

4.4 Plan for continuity and for the claim

Continuity planning for connected fleets should assume the platform is gone entirely rather than degraded. When the state of Missouri lost access to its fleet management environment, agencies went back to telephone processes for vehicle reservations, as described in Chapter 2.

The preparation is inexpensive — actions like periodic export of driver rosters and vehicle assignments, with offline retention of those rosters, preserve the information needed to operate manually. A secondary means of reaching drivers covers the loss of the primary application. Setting the right expectations and agreeing on those with significant customers ensures that the first conversation about missed commitments does not take place during the incident. And as with any recovery plan, these procedures need to be tested rather than assumed.

Recovery depends on records as well. Chapter 3 noted that the available information does not always distinguish mechanical failure, software malfunction, operational error, and malicious activity, and that determination rests on logs and operational data held by platforms and vendors, often under retention periods the business has never looked at. Establishing those retention terms in advance, and knowing how to request preservation, belongs early in incident response rather than late.

Business income loss, as Chapter 3 describes, gets established by reconstructing what the business would have earned if the incident had not happened, along with what it spent to keep operating, and that reconstruction runs on operational records showing what the fleet was committed to before the disruption and what it could not deliver during it. A business that cannot produce those records has not lost less; it has lost the ability to demonstrate what it lost.

These measures are also what an underwriter is able to verify. Account control, vendor diligence, defined escalation, and tested continuity planning are observable practices rather than assertions, which makes the exposure more assessable to underwrite and more straightforward to substantiate at claim.

Conclusion: A Wider View of Connected Vehicle Cyber Risk

A connected vehicle is more than a transportation asset. It can also be an endpoint within a larger operational environment that includes driver applications, fleet management platforms, cloud services, aftermarket devices, customers, and suppliers. A cyber incident affecting any part of this environment may therefore extend beyond the vehicle itself. Disruption does not require compromising a safety-critical function. Losing access to fleet information, connected services, or trusted operational data may interrupt dispatch, deliveries, customer service, and other revenue-generating activities. Shared platforms and services may also allow the effects to extend across multiple vehicles and operations. Automotive cyber risk can consequently reach across vehicles, platforms, businesses, and supply chains.

The resulting loss may include interrupted income and additional expenses for alternative transportation, investigation, restoration, and recovery. Data compromise, extortion, or damage to vehicle systems may result in additional costs. The potential loss cannot always be understood solely from physical vehicle damage.

Understanding this exposure requires three connected perspectives: the business activities that rely on the vehicle, the vulnerabilities and attack paths within its connected environment, and the potential financial consequences. Together, they reveal where risk accumulates and how far an incident may reach.

This exposure is not only more visible when these perspectives are connected. It is materially reducible. Much of what reduces it is not specific to vehicles at all. Account control, vendor diligence, defined escalation, and tested continuity planning are established practices that simply have not been extended to the connected fleet yet. And because they are observable rather than asserted, they also make the risk more assessable to underwrite and more straightforward to substantiate at claim.

As vehicles become more closely integrated with digital operations, automotive cyber risk and enterprise risk are becoming increasingly difficult to separate. The resilience of the vehicle, the business, and its wider commercial relationships is becoming part of the same risk picture.

References

[1] https://vicone.com/company/press-releases/vicone-2026-automotive-cybersecurity-report-cyber-incidents-now-span-entire-organizations/

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

[3] https://www.fmcsa.dot.gov/hours-service/elds/electronic-logging-devices

[4] https://vicone.com/blog/what-commercial-fleet-operators-should-know-about-eld-data-integrity/

[5] https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf

[6] https://vicone.com/blog/securing-smart-transit-lessons-from-a-def-con-bus-hacking-demo/

[7] https://today.ucsd.edu/story/2-million-cars-with-anti-theft-systems-installed-by-dealers-are-at-higher-risk-of-theft

[8] https://www.cve.org/CVERecord?id=CVE-2025-4364

[9] https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-11

[10] https://vicone.com/blog/automotive-cyber-risks-to-watch-from-zero-days-to-ai-backdoors/

[11] https://www.munichre.com/hsb/en/products/cyber-insurance/commercial-cyber-insurance/auto.html

[12] https://content.govdelivery.com/accounts/MOOA/bulletins/411604e

[13] https://www.bbc.com/news/articles/cx2gx28815wo

[14] https://www.nihon-kotsu.co.jp/news/20260713-3334/

[15] https://vicone.com/blog/redefining-risk-why-cybersecurity-is-critical-in-auto-insurance/

[16] https://vicone.com/blog/from-bug-bounty-to-battlefield-what-pwn2own-automotive-reveals-about-real-world-risk/

[17] https://vicone.com/reports/2026-automotive-cybersecurity-report/

[18] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[19] https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

[20] https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

[21] https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident

[22] https://www.reuters.com/business/uks-vertu-motors-sees-up-74-million-hit-jlr-cyberattack-2025-10-08/

Learn more about VicOne by visiting VicOne.com or scanning this QR code: