CYBER RISK FOR VEHICLES

The fast-paced evolution of vehicle automation, combined with increased reliance on internet-connected technologies in critical operations, has the potential to give rise to an increased number of cyber incidents.

Technology & risks

To date, the overwhelming majority of cyber incidents have related to information technology (IT) rather than physical-based processes of operational technology (OT). We now find ourselves at an inflection point where the potential for cyber threats arising from the prolific use of digital systems to control physical processes will bring IT and OT risks closer together.

As vehicles evolve, three different categories of "intelligent" vehicles can be distinguished:

- **Connected vehicles** use technology to communicate with each other, connect with traffic signals, signs and other road items, or obtain data from a cloud.
- **Automated vehicles** use technology to steer, accelerate and brake, with little to no human input.
- **Autonomous/self-driving vehicles**: the difference between automatic (or automated) and autonomous is the degree of human intervention.

To meet the well-known expectations of Elon Musk, who said, "Self-driving cars are the natural extension of active safety and obviously something we should do," there is still a long journey ahead for the motor industry.

All this new technology creates emerging risks to road users. Based on the top 10 security risks for connected cars [as shown below], we can identify three main categories of risks:

1. **Privacy**: The risk of third parties listening in to private conversations while driving–access to personal data.
2. **Security**: The risk of attackers remotely seizing control of a vehicle while in motion.
3. **Safety**: The risk of technology failure, for instance relating to algorithms dictating the application of the brakes.

Chart 1: Top 10 Security Risks for Connected Cars

- **Theft of personal data.** (Personal trip and location data, entertainment preferences, and even financial information)
- **In-vehicle infotainment (IVI) vulnerabilities.** (Everything from satellite navigation to high-definition streaming)
- **Vehicle theft.** (Digital keys, wireless key fobs and mobile applications replacing physical car keys)
- **Connection risks.** (Exploitation of the flaws in a vendor's implementation)
- **Manipulation of safety-critical systems.** (Cruise control system, steering and braking systems)
- **Mobile application security vulnerabilities.**
- **Lack of "designed-in" security.**
- **Security vulnerabilities in the complex supply chain.**
- **Failure to keep up with the latest security patches and updates.**
- **Inadequate key management processes.** (Manual process still used for the management of cryptographic keys)

Source: Guy Carpenter

Various vehicle manufacturers point out the increasing risk of car hacking and admit to vulnerabilities in their software:

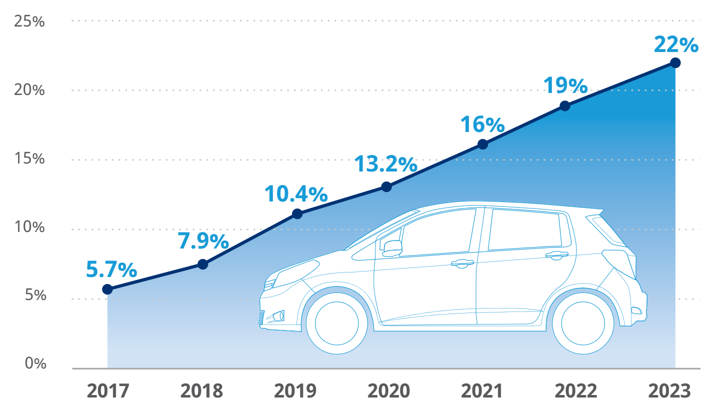
• Motor-vehicle software is often provided by external partners who themselves externalise parts of the software.

• Car manufacturers also use open-source systems such as Linux, Android and FreeRTOS.2 to avoid cost pressures.

• A large number of vehicles often make use of the same software, which increases the concentration of the risk.

In addition, vehicle manufacturers report the cyber risk as realistic with a growing probability of occurrence, particularly with the increasing number of connected cars. According to Statista, the percentage of connected-car stock should increase from 5.7% in 2017 to 22% by 2023:

Chart 2: Connected Car Stock



Source: Statistica, March 2019

Cyber issues and motor coverage

There are two key types of cyber risk exposures:

1. Loss to tangible property including the financial consequences

Liability and property-damage policies take into account exposure to physical loss, bodily injury and consequential damage that result from a covered physical loss. Standard reinsurance programmes protect for this—for the moment.

2. Pure financial loss

Cyber policies are designed to cover non-physical losses that are not a consequence of a covered physical loss. This corresponds to pure financial losses, without infrastructures or information systems being affected (either partial or total destruction).

Chart 3: Two Ways to Cover It: Affirmative vs. Silent

AFFIRMATIVE

Standalone cyber policies

Extensions within non-cyber policies

• Loss of data
• Business interruption and additional cost without physical damage
• Virus
• Computer fraud
• Kidnap & ransom (K&R)
• Directors & officers (D&O)

NON-AFFIRMATIVE (SILENT)

Professional liability
Non consecutive non physical damage
D&O

All risks policies

Problems inherent in the drafting of insurance contracts orginally intended to manage tangible assets and not intangible assets
(Definition of a physical damage)

Wording alignment in insurance and reinsurance

Per risk and accumulation exposure for physical damage and bodily injury

Source: Guy Carpenter

Motor insurance is primarily concerned with non-affirmative (or silent) cyber. Most motor losses that can be expected are:

• Physical damage to the car–theft and vandalism.

• Physical damage and bodily injury through third-party liability.

Legally, we have to distinguish between types of insurance when talking about bodily-injury accident: motor third-party liability (MTPL) versus product liability. We expect a move from third-party to first-party insurance with the increase of technology in cars.

Table 1: **MTPL vs Product Liablility**

MTPL	Product Liability
In the event of an accident (with bodily injury) the **first insurance involved is MTPL** (Badinter law in France, Road Traffic Act in the UK, etc.). Possible recourse against the car manufacturers, car spare-parts suppliers, garages, etc. (e.g., defect on a truck tyre causing a fatal accident). MTPL	Manufacturer's liability can be attracted based on the 1985 European Directive on product liability. Specifics: Manufacturer's liability can be attracted based on the 1985 **European Directive** on product liability. Specifics: • No-fault liability for dangerous product. • Need to prove the default + bodily injury and/or physical damage + causal link. • Principle of denunciation vs recourse (up to the importer of the product in the EC).
• The top cause for any car accident is through human error. • The new technologies released by the motor industry have helped in reducing the number of car accidents. • Car accidents likely will continue to decrease. **Motor liability (r)evolution is expected**: move from third-party to first-party insurance (e.g., no-fault liability in Israel).	Question mark on the very concept of a product: for some, standard software will be a product, while tailor-made software falls under the concept of service. How to apply the concept of defect to software? Indeed, the very nature of software means that it contains bugs, during its start-up period and also during its maintenance in service. **Obligation of means and not of result**

Source: Guy Carpenter

With these points in mind, we set out in the following table the direct impact of these changes for the insurance industry in terms of frequency, severity and accumulations:

Table 2: Aspects of Change and Their Effect on Liability

	MTPL / Personal Accident	Product Liability	General Liability
Frequency	A possible increase in the number of losses due to cyber. Largely compensated by drop in the number of accidents due to human error following increase of driver's safety systems.	Tariff	Possible losses as a result of General Data Protection Regulation (GDPR).
Severity	Unchanged	Unchanged and capped at level of the original policy limit.	Unchanged and capped at level of the original policy limit.
Accumulation	Scenario: takeover of several vehicles that are involved in one or more accidents: • If same accident = 1 event • If several accidents = several events. Not neutral at the reinsurance level—watch out for aggregation clauses.	Possible accumulation through the supply chain.	Possible accumulation through various stakeholders.
Watch out	*Theft / Vandalism*	*Product recall*	

Source: Guy Carpenter

Focus on cyber risk linked to car manufacturers' property insurance

In the case of a malfunction of systems that disrupts the manufacture of vehicles, this could lead to a large business-interruption loss. The reinsurance market after the COVID-19 crisis has strongly limited the application of cyber business-interruption clauses:

- Requiring that their application be linked to physical damage.
- Which in terms of cyber strongly limits the potential risk transfer (or recovery.)

How Guy Carpenter Can Help:
Our Commitment to Addressing Cyber Needs

- Guy Carpenter maintains a cross-territory presence of experts within the mobility spectrum to bring added value to clients.
- As regulators formalize capital requirements and qualitative measurements of risk appetite in this rapidly evolving market, companies will be required to enhance cyber underwriting and reinsurance strategies, leverage innovative modeling capabilities, and develop technical and underwriting risk talent to continue offering clients the best security possible.
- Guy Carpenter's global Cyber Center of Excellence is a dedicated team of brokers, product innovators and analytic experts advancing the role of cyber reinsurance and retrocession. Our Cyber team helps clients achieve profitable growth.