Road Transport Study: Digitalization is Progressing Rapidly, but Cybersecurity Awareness Still in its Infancy

* Cybersecurity gap between the big players and smaller companies
* Relatively high sense of security and modest investments can entail risks
* New cybersecurity regulation is an important step towards more vehicle security
* Adequate solutions for the industry must be further expanded

Schwalbach, Germany, September 2020: While digitalization in the efficiency-driven road transport industry is progressing rapidly in all business areas, the general awareness of the need for protection against cyberattacks is still in its infancy. This is one of the results of “Commercial Vehicles 2020 – Cybersecurity and Digitalization”, a study by the technology company Continental. It is true that connectivity solutions are playing an increasingly important role in the supply chain and in the transportation industry because they increase efficiencies and help cut costs in an increasingly competitive market. “However, connectivity also increases the risks of cyberattacks on transportation companies. At the same time, smaller companies in particular are still hesitant to invest in protecting themselves and their vehicle fleets from attacks,” explains Dr. Mathias Dehm, Head of Research and Processes for Product Security at Continental. Solutions that are more closely tailored to their needs and budgets and the recent regulation of the field of vehicle cybersecurity can greatly improve their cybersecurity posture. For the study, the Institute for Applied Social Science (infas) questioned German experts in associations, authorities, road transport companies and technology service providers using qualitative guideline interviews. The survey was supplemented by an industry panel, for which infas interviewed German road transport companies, logistics experts and trucking companies online.

High sense of security can entail risks

Another result of the study: many companies feel relatively secure from cyberattacks. Around two-thirds of those surveyed on the industry panel consider themselves well protected against such an attack. Only around half of the companies have cyber security mechanisms in place to protect them against a cyber-attack on their logistics or fleet management systems. Three-quarters of the panel are not planning any larger investments within the next six to twelve months. This relatively high sense of security can also entail risks. “Although fleets have not yet been in the limelight in cybercrime discussions, they are attractive targets due to their cargo, such as dangerous goods, their fleet size and their economic importance. Consequently, there is potential danger for logistics companies, for example when criminal hackers shut down fleets to extort ransom money,” says Mathias Dehm.

Cybersecurity protects the benefits of digitalization

“The study shows that cybersecurity is critical, especially for the efficiency-driven road transport sector, since without connectivity it is almost impossible to work efficiently work. Cybersecurity protects the benefits of digitalization, which is vital for the commercial vehicle industry in particular. It therefore deserves more attention,” says Gilles Mabire, Head of the Commercial Vehicles and Services (CVS) business unit at Continental. “In the future, it may well be that the intrinsic value of cybersecurity will become more evident, for example when the increase in digitalization causes more attacks on transport and logistics companies’ systems. This may also increase the willingness to invest,” adds Mabire.

Cybersecurity needs to be affordable for smaller fleets

The rule of thumb generally applies: The larger the company, the higher the awareness of cybersecurity issues. “There is a cybersecurity gap between the few big players and a multitude of smaller companies. Corporations can develop strategies, hire IT and automotive cyber security specialists and set up their own cyber units, but smaller companies often lack the awareness and financial means to do so,” says Dehm. This is a problem, especially in the low-margin logistics sector, where every cent spent on investment counts. According to the latest survey by the German Federal Office for Goods Transport, the industry is dominated by small and medium-sized companies.[[1]](#footnote-2) In addition to legal regulations, companies – and especially smaller ones – will have to be provided with affordable solutions which are customized to match their requirements. “There is no question that cybersecurity must be accessible to all,” said Ido Ben Ami, Vice President Research & Development, Argus Cyber Security. “For this reason, scalable cyber security solutions have been made available to enable small fleets to expand their cyber security capabilities as they grow. For example, a security operations center that enables fleet managers to monitor, detect and respond to attacks can be tailored according to the specific requirements and resources of each organization.”

Cybersecurity requires a holistic view of the company

When it comes to investments in cybersecurity, many companies find it difficult to sustainably use security solutions, since the software is usually regarded as being completed when the programming has been done. However, continuous investment is required to keep the systems up to date, and this can involve customization to match the system environment of the particular company, regular updates, staff training and, last but not least, support. In short, a one-off investment is not enough to address the issue comprehensively and anchor it permanently in the company. “In addition to the trucks themselves, cybersecurity also affects the entire IT, including fleet management systems or the organization of work. If possible, these areas of responsibility should be brought together in a holistic concept so that all interfaces between the areas are covered,” points out Mathias Dehm from Continental.

Uniform cybersecurity standards – an important step towards more vehicle safety

More than three years were spent working on a new regulation to establish uniform cybersecurity standards for vehicles. The regulation drawn up by the Working Party WP.29 of the UN Economic Commission for Europe (UN ECE) examines the security requirements during the vehicle type approval process. In addition to reviewing the appropriate safety measures in place, it also audits company processes among other things. This ensures that cybersecurity is addressed during the development and industrialization of components and software. The UN ECE WP.29 will be introduced in stages starting in mid-2022 and will apply to all newly registered vehicle types in Europe from July 2024 – an important step towards greater vehicle safety. “Given the ever-increasing level of connectivity in areas like automated driving and applications relating to 5G, cybersecurity will continue to gain importance and should therefore always be taken into considereation in new application areas,” says Gilles Mabire.

About the study

For the “Digitalization and Cybersecurity in the Commercial Vehicle Industry” study on behalf of Continental, infas (Institute for Applied Social Science) questioned experts from associations, authorities, transport companies and technology service providers about cybersecurity and the challenges for the transport and logistics industry caused by digitalization. A total of ten qualitative guideline interviews were conducted in open form between December 2019 and February 2020, either by telephone or personally. The survey included questions on topics such as digitalization in the company, the importance of cybersecurity, threats, measures, structures, needs and the desire for improvement. The survey was supplemented by an industry panel, for which infas conducted online surveys of companies in the transport sector, logistics companies and trucking companies. To this end, transport, logistics and trucking companies in Germany were contacted between February and May, using statistical random selection. The evaluated results from the 40 participants provide an insight into the status of the industry’s digitalization, the use of software solutions and the topic of cybersecurity in the commercial vehicle industry.

Continental develops pioneering technologies and services for sustainable and connected mobility of people and their goods. Founded in 1871, the technology company offers safe, efficient, intelligent, and affordable solutions for vehicles, machines, traffic and transportation. In 2019, Continental generated sales of €44.5 billion and currently employs more than 232,000 people in 59 countries and markets.

Continental develops pioneering technologies to make commercial transport safer, more efficient and more connected. The company’s products and services deliver measurable impact for commercial vehicle manufacturers and the aftermarket. They benefit from a broad portfolio and from fully integrated systems. The portfolio includes tires, digital tire monitoring, fleet management, telematic solutions, Electronic Logging Devices (ELD) and tachographs, hoses, air springs, Electronic Control Units (ECU), displays, drivetrain and exhaust aftertreatment systems, sensors, advanced driving assistance systems, as well as eHorizon maps and events and cloud-based services. In 2019, the share of Continental’s global sales for commercial vehicle products, systems and services was €5 billion.

Press contact

Christopher Schrecke

Head of Media Relations

Commercial Vehicles & Services

Continental

Phone: +49 69 7603-2022

E-mail: christopher.schrecke@continental-corporation.com

**Press portal:** www.continental-press.com

**Media center:** www.continental.com/media-center

Images and captions

|  |  |
| --- | --- |
| Continental\_PP\_Study\_Cybersecurity\_Infographics\_I\_Secure\_EN.jpg | The commercial vehicle industry feels relatively secure in terms of cybersecurity and therefore only makes modest investments – a policy that entails risks.  |
| Continental\_PP\_Study\_Cybersecurity\_Infographics II\_SW Update\_EN.jpg | Most fleet companies rely on manufacturers and workshop visits when it comes to keeping the software up to date. Only few have a comprehensive overview as to whether the vehicle software is up-to-date.  |
| Continental\_CV\_Cybersecurity\_wAttacks.jpg | The UN ECE regulation WP.29 for the first time establishes uniform cybersecurity standards for vehicles. In addition, solutions that are tailored more closely to the smaller companies typical of the industry can provide more vehicle security. |
|  |  |

1. <https://www.bag.bund.de/DE/Navigation/Verkehrsaufgaben/Statistik/Ustat/ustat_node.html> [↑](#footnote-ref-2)