KPMG

Cybersecure Vehicles

Growing number of connected vehicles warrants better cybersecurity measures

Automotive Industry Insights

Content

Current situation

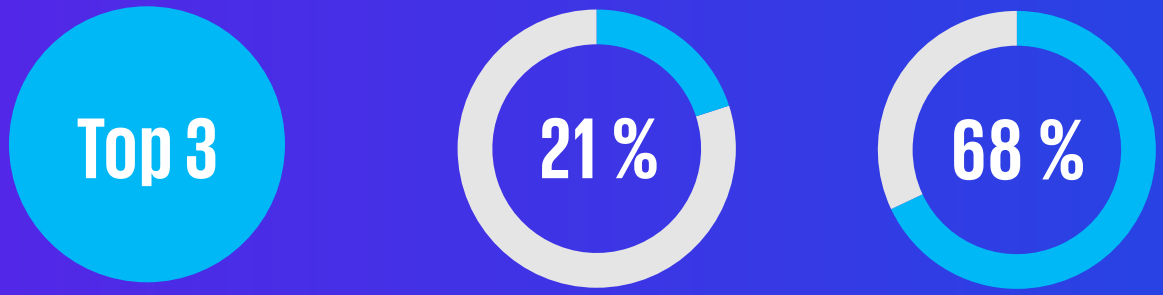
With the advent of electric, autonomous, and connected vehicles, the threat of cyberattacks has risen considerably in the automotive industry. Today's vehicles employ 100 million lines of code powering many technologically advanced systems like intrusion detection and prevention systems, anomaly detection algorithms, communication protocols, over-the-air (OTA) updates, etc. These new digital systems, protocols and algorithms make today's vehicles extremely vulnerable to unauthorized access and hacking of consumer data, and security breaches of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication and telematics systems.

Moreover, when it comes to consumer purchasing decisions as well as consumer trust, data privacy and security plays an extremely important role. In fact, according to KPMG's latest Global Automotive Executive Survey, 21 percent (compared to 40 percent in the previous year) of industry executives believe consumers will trust OEMs to safeguard vehicle data (see Figure 1). Hence, the onus of having adequate cyber-secure systems and processes in place lies with the automotive OEMs.

The main types of cybersecurity threats currently afflicting the automotive industry come in the form of keyless car thefts, EV charging station exploitation, Infotainment system attacks, Brute force network attack, Phishing attacks, Compromised aftermarket devices, Ransomware, and Automotive supply chain attacks[1]. Apart from consumer data, the intellectual property of the automotive organization also lies at risk given the interconnected OT (Operational technology) and IT (Information technology) systems over a corporate network.

Figure 1:

Key insights from KPMG's Global Automotive Executive Survey



purchasing criteria among consumers remains data privacy and security.

of automotive industry executives believe that consumers will trust OEMs to safeguard vehicle data.

of automotive industry executives think that automakers have adequate cybersecurity practices in place.

Source(s): 24th Annual KPMG Global Automotive Executive Survey, 2024

[1] AT&T Business, "The top 8 Cybersecurity threats facing the automotive industry heading into 2023", February 2023

Challenges to overcome

Lack of interdisciplinary cybersecure design and processes

As the manufacturing ecosystem of new automobiles becomes more complex, there is a need to incorporate cybersecurity into the whole lifecycle and value chain of a vehicle - from design to decommissioning. In a typical smart factory configuration, powered by 5G technologies, information - on vehicle production, intellectual property, production schedules, components - can be extremely vulnerable while travelling from OT systems to IT systems over a corporate network. This can result in faulty production quality, disrupted production schedules, theft of intellectual property, and damage to corporate reputation.
Furthermore, as many OEMs focus on launching new models (especially in the EV space), and introduce new vehicle features, they don't give preference to better security and data compliance protocols during the developmental cycle which can leave backdoors open for hackers to exploit.

Increasing regulatory complexity around cybersecurity and data privacy

Regulations by The World Forum for Harmonization of Vehicle Regulations (WP.29), under the UN Economic Commission for Europe (UNECE) - implemented from 2022 onwards in over 60 countries worldwide – requires OEMs and their suppliers to adhere to non-negotiable standards and protocols on cybersecurity and over-the-air software updates. A new amendment to this regulation will require vehicle type approval and even vehicle models under development will need to comply - right from R&D to production to customer end-use[2].
However, many OEMs and suppliers not only have trouble understanding cybersecurity jargon, but also majority of them seem not to have a plan in place for complying with such evolving cybersecurity regulations. This is disconcerting as non-compliance with new regulations can lead to production blackouts and launch delays for new models, seriously eroding the market presence and reputation for OEMs. Thus, establishing permanent transparency on changed legal and regulatory requirements and judging their impacts on business activities remains an enormous challenge for automakers.

Insufficient cybersecurity compliance within the supply chain

A typical passenger vehicle nowadays contains anywhere between 15,000 – 30,000 components involving hundreds of Tier-I, Tier-II and Tier-III suppliers, and is thus an outcome of an increasingly complex supply chain. However, with the supplier management systems implemented by OEMs not being perfect, suppliers within an automotive OEM's network not only lack in their awareness and ability to deal with cyberattacks, but also lack standardized cybersecurity management processes covering whole lifecycle of the vehicle components that they are manufacturing. With the UN155/156 (of UNECE/WP.29) cybersecurity regulation to be implemented by July 2024, the onus of complying with this regulatory framework and non-negotiable minimum requirements will lie with both the OEMs and suppliers which if not followed can lead to heavy fines and losses thus eroding business trust.

Lack of standardized measures for assessing cybersecurity maturity

Although there are many cybersecurity maturity models propagated by industry bodies or specific cybersecurity companies, there is no ONE standardized maturity or assessment model which can not only determine the current and desired state of cybersecurity preparedness for an automotive company, but also benchmark it against its peers. Cybersecurity maturity models are important for automotive companies as it helps them determine at which stage of cybersecurity preparedness they are in, and what further needs to improve. Companies on top of the maturity model curve are "on a continuous cycle of monitoring, evaluation and improvement" that helps them in not only comply with evolving regulations, but also minimize cybersecurity risks to a great extent[3].

[2] CSO, "Automotive supply chain vulnerable to attack as cybersecurity regulation looms", September 2023
[3] Verizon, "Cybersecurity maturity models demystified, and how to implement one", accessed on 17th October, 2023.

Increasing number of internal and external interfaces

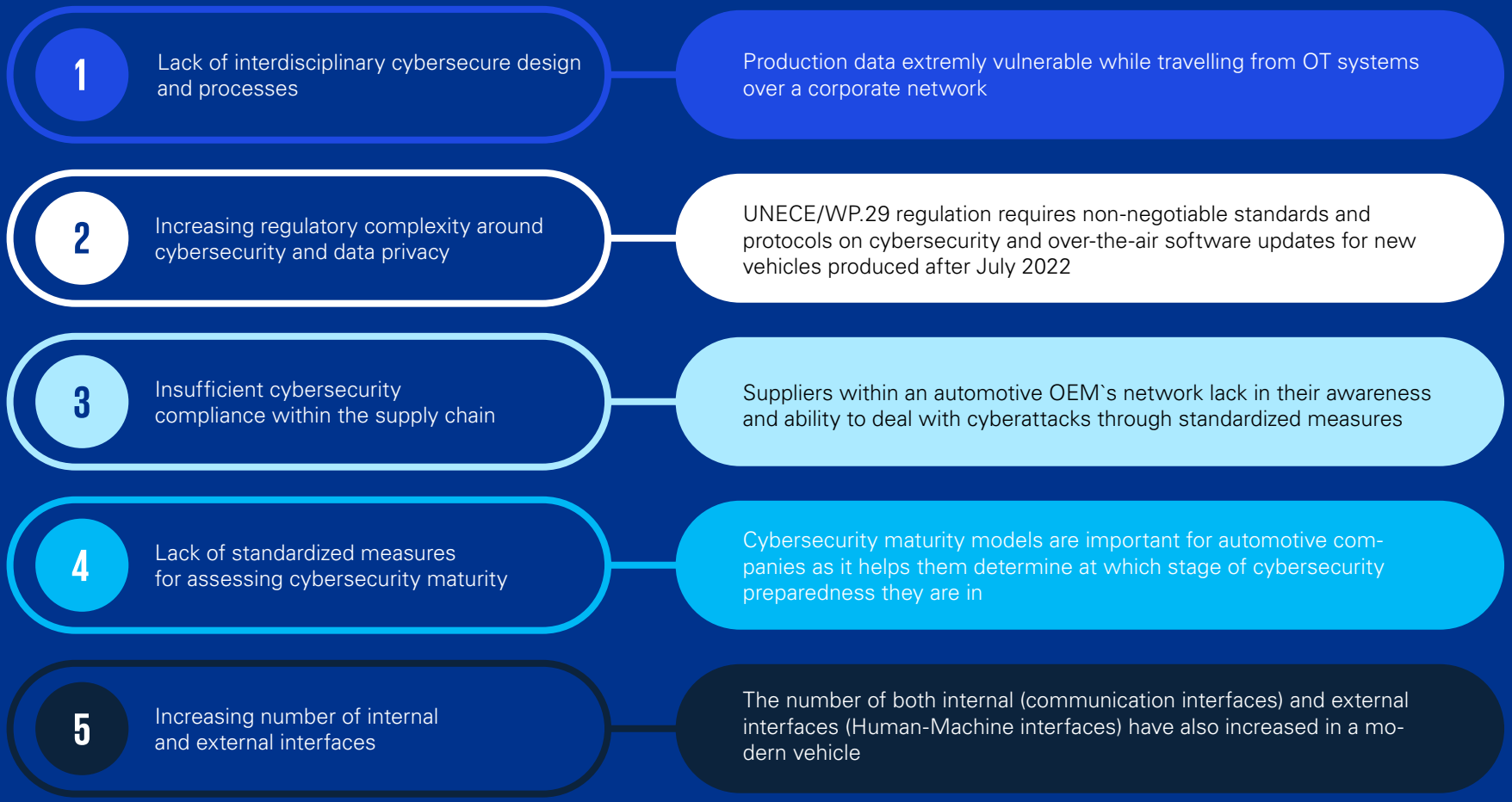
With increasing connectivity and the need for a better in-vehicle consumer experience, the number of both internal and external interfaces have also increased in a modern vehicle. For example, several automotive communication interfaces allow the 150-odd ECUs (Electronic Control Units) in a connected vehicle to communicate and exchange information with one another. Adoption of more advanced navigation and infotainment systems within a vehicle also means that there are a number of Human-Machine Interfaces (HMIs) like Heads-up display, Steering-based controls, Digital instrument clusters, etc., which enhance user experience. With the growing adoption of connected and autonomous vehicles, such interfaces will increasingly become the focal point of cyberattacks if not secured.

> Cybersecurity best practices and maturity models have to be implemented in not just the host automotive organization, but also among its supplier network to ward off cyberthreats and adopt a standardized robust approach to cyberattacks throughout the value chain.

Goran Mazar
Partner
EMA & German Head of ESG and Automotive
KPMG AG Wirtschaftsprüfungsgesellschaft

Figure 2:

Challenges associated with automotive cybersecurity



Source: KPMG in Germany 2024

The way forward

Implement and maintain cybersecurity maturity monitoring

To ensure vehicle cybersecurity, it's crucial for automotive OEMs and TIERs to establish and maintain a Cybersecurity Management System (CSMS). Maturity monitoring of the CSMS plays a pivotal role in tracking compliance with requirements across relevant frameworks and monitoring the progress of implementation. This proactive approach not only saves valuable time and resources but also ensures that organizations remain firmly on the right path.

Set up interdisciplinary teams to manage cybersecurity

Companies need to set up interdisciplinary teams that understand all perspectives ranging from governance topics and engineering-level issues to operational challenges. It is the need of the hour to extend one's cybersecurity capabilities with the help of external service providers. CIOs in automotive organizations should be aware of which cybersecurity services they need to keep in-house and which to outsource. This will also help them determine a standard operating model between the organization and the external service providers.

Stay up-to-date on global legislative changes in cybersecurity and data privacy

The UNECE requirements or Chinese cyber security regulations outline the necessity to proactively monitor legislative changes. The risk of non-compliance can even lead to losing the license to operate business in a country (for example: in case of the China Data Security Law). Constant monitoring of (upcoming) global legislative changes in cybersecurity and data privacy is a must to proactively deal with their impacts.

Reuse not re-invent

A mix of internal and external resources can provide sufficient capacities, leveraging existing knowledge from within the automotive organization, thus integrating industry best practices using proven templates. For example, when it comes to cybersecurity maturity models there are association or government agency-led maturity models that are already out there. Automotive companies can take stock of such cybersecurity maturity models and assess which key process areas (KPAs) or practices in various domains are considered essential to a mature cybersecurity strategy for them.

Manage Cyber risks along the supply chain

Cyber risks need to be managed along the whole automotive supply chain to achieve an organization's target security level, given the UNR155 regulation (part of UNECE/WP.29 regulation) which impacts the whole automotive ecosystem including suppliers. According to this new requirement, automakers will be required to demonstrate how their cybersecurity measures, frameworks and practices will manage dependencies on suppliers, service providers/ vendors, and third-party organizations.

Current experiences

CSMS maturity assessments and implementation for an automotive supplier

Implementation of CSMS maturity assessment: A maturity assessment of the CSMS (Cybersecurity Management System) was carried out employing the KPMG methodology. This assessment aimed to establish compliance with UNR155, ISO/SAE 21434, VDA Rotband, ISO/PAS 5112, OEM requirements, and internal specifications set by the group. The evaluation was facilitated through the utilization of a web-based tool, spanning both the management system and vehicle project levels. This assessment was methodically prepared by defining the relevant scope and conducting 10 interviews with all relevant stakeholders. As a result, the assessment determined adherence to UNR155, ISO 21434, and VDA Rotband standards.

Definition of a roadmap for achieving the target maturity level: Following the CSMS maturity assessment, measures were identified based on the obtained results to achieve the recommended target level. These measures were then consolidated into a roadmap for implementation in projects, providing a clear plan for achieving the desired level of maturity in the CSMS.

Implementation of the measures: Measures were implemented across five dimensions, including Ecosystem Management, Security Governance, Risk Management, Security in Concept & Development, and Security in Production and Operations to achieve the target maturity level for the CSMS. These measures involved the definition and implementation of roles and responsibilities, processes, KPIs and controls, as well as the implementation of methods in vehicle projects such as TARA methodology, Security Testing, Vulnerability Management, and Security Incident Management.

> “
>
> Automotive OEMs should acquire or collaborate with cybersecurity companies to standardize frameworks, assessment methodologies and KPIs across their value chain for them to effectively ensure cybersecurity resilience and further strengthen responses to cyberattacks.
>
> **Jan Stoelting**
> Partner
> Consulting, Automotive & Industrial Manufacturing
> KPMG AG Wirtschaftsprüfungsgesellschaft

UNR155 CSMS implementation for a global Top 5 OEM

Business perspective: The transition of a leading premium car manufacturer to a provider of sustainable and safe & secure mobility requires the implementation of new business models within the existing product ecosystem. The ultimate goal was to achieve sustainable growth through the production of products.

Risk perspective: The potential risks include uncertainties in consumer purchasing decisions, particularly in relation to security-related autonomous functionalities. Non-compliance with regulatory requirements also poses a risk, as it could jeopardize homologation in all markets. Additionally, frequent successful hacking attempts at OEMs, which are often reported in the media, could damage the reputation and brand of the company.

Regulatory perspective: Our developed strategy for the customer covers the implementation and certification processes for both manufacturers and suppliers. There was also a strong focus from international and national authorities on security regulations, particularly in relation to aspects of autonomous driving.

Design of a UNR155/R156 and ISO21434 compliant Vehicle Level Risk Management for a global OEM

A KPMG's expertise in the automotive industry encompasses the successful implementation of two crucial risk management approaches: Threat Analysis and Risk Assessment (TARA) and Vehicle-Level Risk Management. With TARA, the focus is on identifying risks at the functional or ECU level to pinpoint potential vulnerabilities. Simultaneously, KPMG has developed a methodology that allows the aggregation of these risks from the functional level up to the vehicle level. This forms the foundation for a comprehensive assessment of risks throughout the entire vehicle and supports enterprise-wide risk management.

Furthermore, KPMG's cybersecurity team has devised methodologies to compare different vehicle architectures based on their risk profiles. This is critical for making informed decisions regarding safety and security.

Through KPMG's expertise in TARA, the development of risk aggregation methods at the vehicle level, and support in corporate risk management, KPMG has successfully assisted customers in ensuring that their vehicles adhere to the highest standards. KPMG's methodologies for assessing vehicle architectures have empowered its clients to make informed decisions and enhance their competitiveness. This particular project served as an impressive reference for our capabilities in the field of risk management in the automotive industry.

UNR155 and ISO21434 Conformity: Ensuring compliance with UNR155 and ISO21434 is crucial for the cybersecurity of vehicles. To achieve compliance, it is important to analyse the risk management process and identify any gaps in compliance with these standards. Once gaps are identified, action plans have been developed to address those. These action plans include recommendations for improving cybersecurity risk management, secure design and development, and testing and validation. By following these recommendations, the customer has been enabled to ensure that produced vehicles are safe and secure.

Interfaces ISMS, SUMS & CSMS: The identification of interfaces between ISMS, SUMS, and CSMS is fundamental for effective cybersecurity risk management in the automotive industry. KPMG provided consulting services to establish and improve these interfaces. By improving these interfaces, organizations can adequately manage cyber risks and ensure the safety and security of their products.

Key contacts

Goran Mazar
Head of ESG &
Automotive in EMA,
KPMG International Partner,
KPMG in Germany

T +49 69 9587-4451
gmazar@kpmg.com

Jan Stoelting
Partner and
Cybersecurity Lead,
KPMG in Germany

T +49 69 9587-6273
jstoelting@kpmg.com

Bernhard Christoph Lang
Partner, Consulting
Automotive & Industrial
Manufacturing
KPMG in Germany

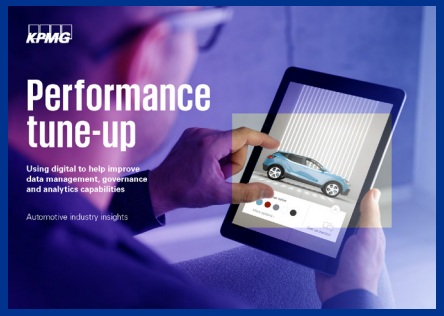
T +49 711 9060-41127
bernhardlang@kpmg.com

Further Publications

Vulnerable supply

Using an ESG and tech based approach to secure the future of supply chains

Read more



Performance tune-up

Using digital to help improve data management, governance and analytics capabilities

Read more

Sustainable Batteries

Uptick in EV battery market depends on a meaningful shift to a circular economy

Read more

www.kpmg.de

www.kpmg.de/socialmedia